ALGEBRA

LECTURES DELIVERED TO POST-GRADUATE STUDENTS OF
CALCUTTA UNIVERSITY

BY

FRIEDRICH WILHELM LEVI, DR. PHIL. NAT.
HARDINGE PROFESSOR

CALCUTTA UNIVERSITY
CENTRAL LIBRARY

PART II

GENERAL ALGEBRA

511·4
·036

PUBLISHED BY THE
UNIVERSITY OF CALCUTTA
1937

BCU 1740

104.707

PRINTED AND PUBLISHED BY BHUPENDRALAL BANERJEE
AT THE CALCUTTA UNIVERSITY PRESS, SENATE HOUSE, CALCUTTA.

Reg. No. 1018B—April, 1937—E

PREFACE

The reasons why these lectures are being published as a provisional edition in different parts have been explained in the preface to the first part, and I have only to refer to it.

This second part deals with General Algebra, *i.e.*, algebra in arbitrary fields. It cannot be expected to find the whole of this theory discussed in these few pages. It was necessary to restrict the subject, and the restriction has been so chosen that the notions of ideal and of non-commutative group have been avoided. Readers interested in this part of mathematics may be referred to van der Waerden, Moderne Algebra (Berlin, J. Springer, 1930-31).

The publication of this second part was only possible by the collaboration of the authorities of the Calcutta University ; so I repeat my heartiest thank to the Vice-Chancellor, Syamaprasad Mookerjee, Esq., M.A., B.L., Barrister-at-Law, M.L.A., for his interest in the teaching and the research of Higher Mathematics and especially for his help on this occasion.

Proofs and manuscript have been revised by Mr. A. C. Choudhury, M.Sc., and I thank him very much for his valuable collaboration. I thank also the Calcutta University Press for the quick and careful printing.

CALCUTTA, ASUTOSH BUILDING.

MARCH, 1937.

F. W. LEVI.

CALCUTTA UNIVERSITY CENTRAL LIBRARY

INDEX

Page.

§ 1. Principal Notions 1

1. Formal laws of calculation. 2. Moduls. 3. Partition in classes. 4. Singular elements. 5. Distributive operations. 6. Submoduls. 7. Systems of double composition and rings.

§ 2. Fields 8

1. Definitions. 2. Homomorphism and Isomorphism. 3. Homomorphism of a system of double composition generated by a partition into classes. 4. Characteristic. 5. Subfields. 6. Quotientfields. 7. Fields of characteristic 0.

§ 3. Polynomials 14

1. Calculation with polynomials. 2. The ring $S[x]$. 3. Integral rational functions. 4. Derivates. Euler's formula.

§ 4. Factorisation 19

1. Fundamental notions. 2. Factorisation of integral numbers. 3. Highest common factors. 4. Functions $N(a)$. 5. The algorithmus of h. c. f. 6. Main properties of uniquely factorisable rings. 7. The algorithmus of division.

§ 5. Extension of a field 27

1. Extensions. 2. Algebraic and transcendental extensions. 3. Fundamental theorem of general algebra. 4. Modul over a field. 5. Fields finite over a field. 6. Finite extensions. 7. Separable and non-separable extensions. 8. Algebraic extensions. 9. Extension by roots of irreducible polynomials.

§ 6. Normal extensions of a field 37

1. Extension of an isomorphism. 2. Normal extensions of a field. 3. Reduction of an irreducible polynomial by a normal extension.

§ 7. Cyclotomic equations 39

1. The nth roots of the unitelement, non-separable case. 2. The Separable case, primitive roots. 3. Cyclotomic polynomials.

§ 8. Galois fields 42

1. Definition. 2. Existence-theorem. 3. Separability. 4. Application on the theory of numbers.

§ 9. Primitive elements of separable extensions 46

Page.

§ 10. Symmetric polynomials 47

1. Elementary symmetric polynomials, their algebraic independence. 2. Representation by sums of monomials. 3. Main theorem. 4. Alternating polynomials. 5 The highest common factor of symmetric polynomials. 6. Power sums.

§ 11. The Field $R(i)$ 53

§ 12. Irreducibility of Polynomials 55

1. Reducibility in a ring of unique factorisation and in its quotientfield. 2. Eisenstein's Theorem. 3. Irreducibility of the cyclotomic polynomials. 4. Irreducibility of a determinant.

§ 13. Closed fields 60

Criterion for a closed field. 2. Fundamental theorem of classical Algebra.

§ 14. Solutions of algebraic equations 63

1. The notion of solution. 2. An elementary reduction. 3. The case $n=2$. 4. The case $n=3$. 5. The case $n=4$.

CORRECTIONS TO PART I.

Page	*Line*	*Read*	*For*
2	10	a_2	a_s
6	13	a^i	a_i
11	15	$\neq 0$	$=0$
18	17	$L(\overset{i}{e}{}^{1}, \ldots, \overset{i}{e}{}^{n})$	$L(\overset{1}{e}, \ldots, \overset{n}{e})$
21	25	The second factor	The first factor
,,	26	the first factor	the second factor
27	Formula (43)	$i \neq r$ and $i \neq s$ belong to their respectively preceding lines	
28	10	of	or
,,	Add : From this diagonal-matrix we get A by the inverse row- and column-additions.		

§ 1. PRINCIPAL NOTIONS.

Let $$a,\ b,\ c,\ \ldots\ldots\ldots\ldots \tag{1, 1}$$ [1/1]

be arbitrary numbers; then there exists, to every pair of numbers, a uniquely defined number s called the *sum*,

$$a+b = s \tag{1,2}$$

and a uniquely defined number p called the *product*

$$a.b = ab = p \tag{1, 3}$$

The operations for the determination of the sum and the product are called the *addition* and the *multiplication*.

For these operations the following laws hold:

Commutative laws:

$$a+b = b+a \tag{1, 4a}$$

$$a.b = b.a, \tag{1, 4m}$$

Associative laws:

$$(a+b)+c = a+(b+c) \tag{1, 5a}$$

$$(a.b).c = a.(b.c), \tag{1, 5m}$$

Laws of inverse existence: *To every pair* a, b *there exists an* x *such that*

$$x+a = b, \tag{1, 6a}$$

To every pair a, b, *satisfying the condition*

$$a \neq 0 \tag{1. 6o}$$

there exists an y *such that*

$$y.a = b, \tag{1, 6m}$$

Distributive law:

$$(a+b).(c+d) = ac+ad+bc+bd \tag{1, 7}$$

These formulae are fundamental in calculation with numbers but they are not sufficient to define numbers. Of course, this word is used in a different manner in the different parts of mathematics. We will consider some systems of numbers for which the formulae (1, 2) to (1, 7) are satisfied.

1. The set of all rational numbers. ✓
2. The set of all real numbers.[1] ✓
3. The set of all complex numbers. ✓
4. The set of all numbers $a_1 + a_2\sqrt{2}$, a_1 and a_2 being rational numbers.

The reader may verify that in each of these systems an element of the same system will be generated by addition, subtraction, multiplication and division, the divisor being $\neq 0$; the commutative, associative and distributive laws hold, because they are satisfied for all numbers.

It is easy to construct other systems of numbers satisfying the conditions (1, 2) to (1, 7), but we will consider arbitrary systems of elements—not necessarily numbers—satisfying these conditions. As in these conditions the number 0 has been used, it will be necessary to replace this number by a suitable element of the system under consideration.

[1/2] A system of elements (1, 1) for which an operation (1, 2) satisfying the conditions (1, 4a), (1, 5a), (1, 6a) is defined, is said to form an *abelian group* or a *modul*.[2] The examples 1, 2, 3, 4 of [1/1] are instances of moduls, but there are also other moduls for which a multiplication is not defined, or the conditions for the multiplication do not hold. *E.g.*, the integers form an abelian group, but (1, 6m) does not hold. The vectors of an arbitrary vector-space (see I, p. 6), form a modul; in this case the elements are not numbers, and the multiplication of two elements is not defined. The 3-vectors are in (1, 1)-correspondence to the parallel displacements of the space, because in a parallel-displacement the vector joining the original point with the image point is the same for every point; hence this vector corresponds to that displacement. If the 3-vectors α and β correspond to the displacements A and B, then $\alpha + \beta$ corresponds to the transformation of the space we get on making the displacements A and B one after the other. So we get, to every vectorspace, a corresponding modul whose elements are parallel-displacements.

---

[1] The theory of real numbers will be given in the lectures on analysis.

[2] There is no essential difference between the meaning of the two words. The term "addition" and the sign + are only notations and there is no harm to replace them by other words. In these cases it is not usual to speak of "moduls," and the word modul is replaced by "abelian group."

Another kind of transformations of the space forming a modul are the rotations about a fixed axis. This modul has a certain connection with the modul of the real numbers. Every real number κ corresponds to a rotation through the angle κ, and two rotations through the angles κ and λ taken one after the other, generate a rotation through the angle $\kappa+\lambda$. Two real numbers α and β correspond to the same rotation if and only if $\alpha-\beta = 2k\pi$, k being an arbitrary integer. Therefore the real numbers have with the rotations about a fixed axis, an $(\infty, 1)$-correspondence for which the addition holds. In order to generate another modul, we apply this method of correspondence to the modul of the integers. For this purpose, we have to replace π by an integer g, and we get a partition of the integers into classes of *congruent* numbers, two numbers a, b being congruent

$$a \equiv b \pmod{g} \tag{1, 8}$$

when $a-b$ is a multiple of g. These classes form a modul, which will be considered below.

In the example just before, a partition of the set of all integers in classes has been generated by a congruence of its elements. We will generalise this consideration. [1/3]

An arbitrary set A of elements a, b, c,...... may be decomposed in classes, so that every element belongs to one and only one class. Two elements are said to be *equivalent* $a \backsim b$ if they belong to the same class. Then the equivalence has the following properties:

$$\begin{array}{llll} 1. & a \backsim a & \text{law of reflexivity.} & \\ 2.\ \text{If} & a \backsim b, \text{ then } b \backsim a & \text{law of symmetry.} & (1, 9) \\ 3.\ \text{If} & a \backsim b,\ b \backsim c, \text{ then } a \backsim c & \text{law of transitivity.} & \end{array}$$

The converse is the following proposition, often used as lemma,

Lemma. If there is an equivalence between the elements of A satisfying the conditions (1, 9), and (a), (b), (c), ... are the classes of the elements equivalent respectively to a, b, c,...., then each element of A belongs to a class, and two classes have either all elements in common,—*i.e.*, they are identical—or they have no common element.

Proof. From 1, it follows that a belongs to (a). If b is a common element of (a) and (c), then it follows from 2, that a and c belong to (b).

From 3, it follows that each element of (a) and of (c) belongs to (b), and that each element of (b) belongs to (a) and to (c) Therefore (a), (b) and (c) are identical.

Each element will be called its representative, and we will use the notation:

$$(a) = \text{the class represented by } a. \tag{1, 10}$$

The congruence (mod. g) defined by (1, 8) is an equivalence satisfying obviously the conditions (1, 9). This congruence generates a partition into g *classes of residues*

$$(0),\ (1),\ \ldots,\ (g-1). \tag{1, 11}$$

Because each integer is congruent to its residue after division by g, we have $(a) = (a')$ if and only if $a \equiv a'$ (mod. g), and if $(a) = (a')$, $(b) = (b')$, $a' = a + r.g$, $b' = b + s.g$, hence

$$\begin{aligned}(a) + (b) &= (a + b) \\ (a)\,.\,(b) &= (a.b)\end{aligned} \tag{1, 12}$$

the right sides being independent of the choice of the representatives in (a) and in (b). From (1, 12) it follows directly:

$$(a) + (b) = (b) + (a),\quad [(a) + (b)] + (c) = (a) + [(b) + (c)].\quad (a) + (b-a) = (b)$$

$$(a)\,.\,(b) = (b)\,.\,(a),\quad [(a)\,.\,(b)]\,.\,(c) = (a)\,.\,[(b)\,.\,(c)],$$

$$[(a) + (b)]\,.\,[(c) + (d)] = (a).(c) + (a).(d) + (b).(c) + (b).(d).$$

Hence the classes of residues (mod. g) form a modul in which a second operation, the " multiplication " is defined satisfying the conditions (1, 4m), (1, 5m) and (1, 7).

[1/4] Let a and b be arbitrary elements of a fixed modul M, then there exist in M elements 0 and c such that

$$\begin{aligned}a + 0 &= a \\ c + a &= b,\end{aligned} \tag{1, 13a}$$

hence $\quad b + 0 = (c + a) + 0 = c + (a + 0) = c + a = b.$

As b is an arbitrary element, we see that each element of M remains unchanged by the addition of 0.

Let $\bar{0}$ be another element, so that $a+\bar{0} = a$, then $\bar{0}$ has the same properties as 0, and the elements of M will not change, when $\bar{0}$ will be added. Hence $0+\bar{0} = 0$, but on the other hand $0+\bar{0} = \bar{0}$ holds. Hence $0 = \bar{0}$.

Theorem. In a modul M there exists one and only one *singular* element, such that for every element a of M, $a+b$ equals (or not equals) a, if b is the singular (or a non-singular) element.

There exists in M an element a', such that

$$a+a' = 0 \tag{1, 14}$$

Let $c+a = \underline{\bar{c}+a} = b$, then

$$c = c+0 = c+(a+a') = b+a' = (\underline{\bar{c}+a})+a' = \bar{c}+\bar{0} = \bar{c}.$$ Hence:

Theorem. The equation $x+a = b$ has one and only one solution. The addition of a' is the operation inverse to the addition of a.

We will therefore call the addition of a' the *subtraction* of a, and we [1/5]
will use the following notations :

$$a' = -a$$

$$d+a' = d-a \tag{1, 15}$$

Therefore $-(-a) = a$ holds (1, 16)

As $(a_1+a_2)+a_3 = a_1+(a_2+a_3)$, we can omit the brackets in this sum.

By mathematical induction we can prove in the same manner, as it is done in elementary arithmetic, that the brackets in the sums of n elements can be omitted.

In place of $a_1+a_2+\ldots+a_n$ we will write sometimes

$$\sum_{i=1}^{n} a_i \;;$$

If $a_1 = a_2 = \ldots = a_n = a$, the sum will be denoted by

$$na. \tag{1, 17}$$

n is therefore a positive integer, and not necessarily an element of M.

We will define the product of a non-positive integer with an arbitrary element a of M by

$$(-\mathrm{n})\,a = -(\mathrm{n}a) = \mathrm{n}(-a)$$

$$0\,a = 0 \qquad (1,\ 17')$$

Hence for all integers p, q the following distributive laws hold :

$$\mathrm{p}a + \mathrm{q}a = (\mathrm{p}+\mathrm{q})a$$

$$\mathrm{p}(a+b) = \mathrm{p}a + \mathrm{p}b.$$

This multiplication is a special case of an operation we will define now.

distributive operation

Let χ be a transformation of M such that

1. if a is an element of M, then χa is also an element of M.
2. $\chi(a+b) = \chi a + \chi b$.

As $\chi a = \chi(a+0) = \chi a + \chi 0$,

$$\chi 0 = 0 \qquad (1,\ 18)$$

holds for every distributive operation.

A vector space is a modul with distributive operations, these being multiplication with real numbers. Later on we will generalize the notion of vectorspace by introducing another set of distributive operations.

[1/6] A subset M' of a modul (abelian group) M is said to be a *submodul* (*subgroup*) of M' if it forms a modul with respect to the addition[1] defined in M.

Theorem. A subset M' is a submodul of M, if and only if the differences of the elements of M' belong to M'.

Proof. The condition is obviously necessary. That the condition is sufficient may be seen from that if the condition holds, and if a and b are elements of M', then $b-b = 0$, $0-b = -b$, $a-(-b) = a+b$ also belong to M'. Hence the addition defined in M can be carried out in M'; for this addition the associative and the commutative laws hold, and the equation $x+a = b$ can be solved by the element $b-a$ of M'. Hence M' is a submodul of M.

---

[1] See footnote, p. 2.

[1/7] Let Σ be a set of more than one element for which an "addition" and a "multiplication" are defined ; it may be supposed that the commutative law (1, 4a) holds for the addition, that the associative law (1, 5a), (1, 5m) holds for the addition and for the multiplication, that the sum (1, 2), and the product (1, 3) of each pair of elements of Σ belong to Σ, and that the distributive law (1, 7) holds. If these conditions are satisfied, Σ is said to form a *System of double composition*.* In a system of double comp. (1, 4a) commu.? for addition absent.

If in a system of double composition Σ, each pair of elements has a difference belonging to Σ, this system is called a *Ring*, and if in a ring the multiplication satisfies the commutative law (1, 4m), the ring is said to be a *Commutative ring*.

A ring can be considered as a modul with distributive operations, these operations being the multiplication—from the left, and from the right hand—with elements of the ring itself.

E.g. The classes of residues (mod. g) form a commutative ring. The Quaternions[1] with integral co-ordinates form a non-commutative ring. The positive integers form a system of double composition.

A subset of a ring R, which itself is a ring with the addition and the multiplication, as defined in R, is said to be a *Subring* of R.

Theorem. A subset R' of a ring R is a subring of R, if and only if the differences and the products of the elements of R' belong to R'. ✓

Proof. The condition is obviously necessary. If the condition holds, it follows from [1/6] that R′ is a modul, and the multiplication in this modul—from the left, and from the right hand—with elements of R' are distributive operations ; hence R' is a ring.

As in a ring the multiplication is a distributive operation, we can apply (1.18) to the left hand and to the right hand multiplication ; hence :

$$c0 = 0 \qquad (1, 13m)$$

$$0c = 0.$$

Therefore it is impossible to satisfy the condition (1, 6m) in any ring without restriction. If we want to introduce the condition that, to every pair of elements a, b there should exist an y, such that

$$y\,a = b \qquad (1, 6m)$$

---

[1] The knowledge of the quaternions is not essential for the understanding of this chapter.

we are compelled to make the restriction

$$a \neq \mathit{0}. \tag{1, 6_{0}}$$

We get this restriction $(1,\ 6_{\mathit{0}})$ from the restriction $(1,\ 6_0)$ used in [1/1] on replacing the number 0 by the singular element $\mathit{0}$ of the modul R.

§ 2. FIELDS.

[2/1] A commutative ring for which the condition (1, 6m) with the restriction $(1.\ 6_{\mathit{0}})$ holds, is said to be a *Field*. In other words: A field is a set of more than one element in which an addition (1, 2) and a multiplication (1. 3) are defined and the conditions (1, 4a), (1, 4m), (1, 5a), (1, 5m), (1, 6a), (1. 6m) with (1.6_{0}) and (1, 7) hold.

Theorem. If a, b are elements of a field F and $ab = \mathit{0}$, then at least one of the factors a, b, must be equal to $\mathit{0}$.

Proof. Let $a \neq \mathit{0}$. $b \neq \mathit{0}$. From (1, 6m). $(1,\ 6_{\mathit{0}})$ it follows that there is in F an element c such that $cb \neq \mathit{0}$, and an element y such that $ya = c$.

Then: $\mathit{0} = y\mathit{0} = yab = cb \neq \mathit{0}$. contradiction.

From this theorem it follows, that the elements $\neq \mathit{0}$ of a field F form a system Σ where the multiplication is commutative and associative. If a and b are elements of Σ, the equation $ax = b$ must have a solution in F, and as $x \neq \mathit{0}$, x is an element of Σ. Hence the multiplication satisfies in Σ the same conditions that the addition must satisfy in a modul; only the sign of + has been replaced by the notation of the multiplication. We can "translate" the results of [1/5] from the "additive language" into the "multiplicative language." From [1/4] there follows the existence of a *singular* element $\mathit{1}$ satisfying the condition

$$a\mathit{1} = \mathit{1}a = a \tag{2, 1}$$

for every element a of Σ. But, as (2, 1) holds also for $a = \mathit{0}$, the following theorem holds:

Theorem. There is one and only one element $\mathit{1}$ in a field satisfying (2, 1) for every element a of the field.

To every element of Σ there is an element a^{-1} satisfying

$$a\, a^{-1} = a^{-1}\, a = \mathit{1} \tag{2, 2}$$

On translating the theorem of [1/3] into the "multiplicative language" we get

Theorem. If a and b are elements of a field F, $a \neq 0$, then the equation $ax = b$ has one and only one solution in F $x = a^{-1}b$.

Corresponding to the sum of n elements we can form the product $\prod_{i=1}^{n} a_i$ of n elements, and if the elements are all equal, we get the *power*

$$a^n. \tag{2, 3}$$

The powers with non-positive integer exponents are defined by

$$a^0 = 1, \qquad (a^n)^{-1} = (a^{-1})^n = a^{-n}.$$

For every pair of integers p, q the equation

$$a^p a^q = a^{p+q} \tag{2, 4}$$

holds.

The necessary and sufficient conditions, that a field must satisfy, can also be given in the following manner:

A system F of more than one element, for which the addition (1, 2) and the multiplication (1, 3) are uniquely defined, is a field, if and only if

1. The elements form a modul; the singular element may be denoted by 0.

2. The elements different from 0 form an abelian group with respect to the multiplication.

3. $a0 = 0a = 0$ for arbitrary elements a, b, c of F

4. $a(b+c) = ab + ac$

The singular element 0 of the modul will be called the *nullelement*.
The „ „ 1 „ „ multiplicative abelian group „ „ *unitelement*.

As there exists in F at least one element $a \neq 0$, and therefore $a1 \neq 0$,

$$1 \neq 0 \tag{2, 4}$$

[2/2] Let the elements $a, b, c, \ldots$ of an arbitrary system Σ of double composition be represented by elements

$$\alpha(a),\ \alpha(b),\ \alpha(c),\ \ldots$$

of a set A, and let in A an addition and a multiplication be defined satisfying the conditions

$$\begin{aligned} &\alpha(a) + \alpha(b) = \alpha(a+b), \\ &\alpha(a)\,\alpha(b) = \alpha(ab) \text{ for all elements } a,\ b \text{ of } \Sigma, \end{aligned} \tag{2, 5}$$

then the representation is said to be a *homomorphism* and A is said to be *homomorphic* to Σ.

Theorem. If Σ is a ring, A is also a ring. If Σ is a commutative ring, A is also a commutative ring.

Proof. Every element of A is of the form $\mathfrak{a}(a)$, where a is a suitable element of Σ not necessarily defined uniquely by its " image" $\mathfrak{a}(a)$.

$$[\mathfrak{a}(a)+\mathfrak{a}(b)]+\mathfrak{a}(c)=\mathfrak{a}(a+b+c)=\mathfrak{a}(a)+[\mathfrak{a}(b)+\mathfrak{a}(c)]$$

$$\mathfrak{a}(a)+\mathfrak{a}(b)=\mathfrak{a}(a+b)=\mathfrak{a}(b)+\mathfrak{a}(a).$$

Hence A is a modul. In the first equation we can replace the sign $+$ by the notation of the multiplication. If Σ is a commutative ring, we can carry out the same replacement in the second equation also. Hence the proposition holds.

As $\mathfrak{a}(a) = \mathfrak{a}(a+0)=\mathfrak{a}(a)+\mathfrak{a}(0)$, the nullelement of A is

$\mathfrak{a}_0 = \mathfrak{a}(0)$. Hence

$\mathfrak{a}_0 = \mathfrak{a}(a-a) = \mathfrak{a}(a)+\mathfrak{a}(-a)$; hence

$\mathfrak{a}(-a) = -\mathfrak{a}(a)$.

In the same manner we get the formulas

$$\mathfrak{a}(na) = n\,\mathfrak{a}(a), \qquad \mathfrak{a}(a^n)=[\mathfrak{a}(a)]^n. \tag{2, 6}$$

From $\mathfrak{a}(a) = \mathfrak{a}(b)$, it follows that $\mathfrak{a}(a-b)=\mathfrak{a}_0$, and that for every element c of Σ $\mathfrak{a}(c)=\mathfrak{a}(c+[a-b])$ holds. Hence :

Theorem. Either every element of A is image of more than one element of a ring R, or every element of A is image of one and only one element of R. In the second case A is said to be *isomorphic* to R, and the homomorphism is an *Isomorphism*.

If A and Σ are isomorphic and form the same set in which the addition and the multiplication have been defined, this isomorphism is called an *Automorphism*. Hence an automorphism is a permutation of elements for which additon and multiplication hold.

Examples : 1. The ring of the classes of residues (mod. g) is homomorphic to the ring of the integers. 2. In the ring of the numbers

$a + b\sqrt{2}$ (a, b integers) the transformation $a + b\sqrt{2} \longrightarrow a - b\sqrt{2}$ is an automorphism.

If α is a homomorphism of a ring R, there is a partition of the elements [2/3] of R in classes, two elements a and b being equivalent if $\alpha(a) = \alpha(b)$, *i.e.*, if $\alpha(a-b) = \alpha_0$. The elements c for which $\alpha(c) = \alpha_0$ form a subring R' of R, with the property that each product of an element of R and an element of R' belongs to R'. The converse of this theorem holds also: Every subring R' of R, having this property, generates a homomorphism of R. This proposition is included in the following theorem :

Theorem. Let Σ be a system of double composition. Let I be a subset of Σ, such that $s+t$, sa and as are elements of I if s and t are elements of I and a is an element of Σ ; let two elements a and a' of Σ be considered equivalent, if and only if there are in I elements s and t such that $a + s = a' + t$; then this equivalence generates a partition of Σ into classes, and the representation of each element a by its class (a) is a homomorphism.

Proof. The equivalence satisfies, obviously, the laws of reciprocity and symmetry ; if $a \backsim a'$, $a' \backsim a''$, there are elements r, s, t, u of I such that $a + r = a' + s$, $a' + t = a'' + u$ therefore $a + (r+t) = a'' + (s+u)$, and $a \backsim a''$. Hence the equivalence generates a partition of Σ into classes. Let $b \backsim b'$, $b + v = b' + w$, v and w being elements of I. Then

∵ r+t
s+u
are
of I

$$(a+b) + (r+v) = (a'+b') + (s+w) \text{ and } (a+r)(b+v) = (a'+s)(b'+t) \ ;$$

therefore $ab + \bar{r} = a'b' + \bar{s}$; $\bar{r} = r(b+v) + av$ and $\bar{s} = s(b'+t) + a't$ being elements of I ; hence $a + b \backsim a' + b'$, $ab \backsim a'b'$. The definitions of addition and multiplication of classes $(a) + (b) = (a+b)$, $(a)(b) = (ab)$ are therefore independent of the choice of the representatives, and the representation of each element by its class generates a homomorphism of Σ.

Remark. The class (0) is composed by the elements of I and those elements, which are differences of elements of I. If Σ is a ring containing I, the negative of each element of I is contained in I too, and I is a ring (of a special type). In this case the classes (a) are said to be *classes of residues* of I in Σ. This definition tallies with the definition given in [1/3] for the special case of integers. In this case Σ is the ring of all integers, and I is the subring of the integers divisible by g.

By (1,17) and (1.17′), $\bar{n}a$ has been defined for elements a of $\overset{g-}{a}$ [2/4] modul. Let us now introduce for fields the notation

$$\bar{n}1 = n \tag{2, 7}$$

The elements (2, 7) form a ring homomorphic to the ring of the integral numbers. Therefore

$$\bar{n}a=na, \tag{2, 8}$$

If $na=ma$, $a\neq 0$ then $(n-m)a=0$, hence by [2/1] $n-m=0$ holds, and for every integer $\bar{q}$, $q(n-m)=0$. Let $g=0$. $\bar{p}$ be the smallest positive integer such that $p=0$, $\bar{g}=k\bar{p}+\bar{r}$, $0\leq \bar{r}<\bar{p}$. By [2/1] we know that $1\neq 0$; hence $\bar{p}\neq 1$. As $r=0$, it follows from the definition of $\bar{p}$ that $\bar{r}=0$. Hence $ma=na$ if and only if $\bar{m}-\bar{n}$ is a multiple of $\bar{p}$, this number being independent of a. Let $\bar{p}=\bar{s}\bar{t}$, then $st=0$; therefore $s=0$, or $t=0$ hence $\bar{s}$ or $\bar{t}$ is divisible by $\bar{p}$ and therefore equal to $\pm\bar{p}$. As $\bar{p}$ has no other positive divisor than $\bar{p}$ and 1, and as $\bar{p}\neq 1$, $\bar{p}$ is a prime number. Therefore:

Theorem. If $\bar{m}a=\bar{n}a$, $\bar{m}\neq\bar{n}$, for an arbitrary element $a\neq 0$ of a field F, then there exists a prime number $\bar{p}$, such that $\bar{m}'b=\bar{n}'b$ holds for each element of F if and only if $\bar{m}'-\bar{n}'$ is divisible by $\bar{p}$.

The prime number $\bar{p}$ is called the *characteristic* of F. If the elements $\bar{m}a$ are all different, then F has the characteristic 0. The fields mentioned in [1/1] are of characteristic 0. The existence of fields of characteristic $\bar{p}$ will be shown in [2/5].

[2/5] When the subset F' of the field F is a field with the addition and the multiplication defined in F, then F' is a *subfield* of F.

We will denote $F'\subseteq F$ when F' is a subfield of F, and if the subfield F' is different from F we will denote $F'\subset F$. Every $F'\subseteq F$ must contain $0, 1$ and therefore $1+1=2, 3, \ldots, n, \ldots$. Let F be of characteristic $\bar{p}$, then $m=n$ if and only if $\bar{m}-\bar{n}$ is a multiple of $\bar{p}$, *i.e.*, if $\bar{m}\equiv\bar{n}$ (mod. $\bar{p}$). There are therefore only $\bar{p}$ different elements corresponding to the $\bar{p}$ classes (mod. $\bar{p}$). $m+n$ corresponds[1] to $(\bar{m}+\bar{n})$, and mn to $(\bar{m}\bar{n})$. Hence the $\bar{p}$ elements form a ring isomorphic to the ring of classes (mod. $\bar{p}$). We will prove that (1, 6m) with the restriction (1, 6_s) is satisfied and therefore the $\bar{p}$ elements form a subfield of F. $mn=qn$ holds if and only if $(\bar{m}-\bar{q})\bar{n}\equiv 0$ (mod. $\bar{p}$). If $(\bar{n})\neq 0$, this congruence holds only if $\bar{m}-\bar{q}\equiv 0$ (mod. $\bar{p}$), *i.e.* if $(\bar{m})=(\bar{q})$. Hence if we multiply the $\bar{p}-1$ classes $(1), (2), \ldots, (\bar{p}-1)$ with $(\bar{n})\neq(0)$, we will get $\bar{p}-1$ different classes, different from $(0)=0$; *i.e.* every class $(b)\neq(0)$ occurs once. The equation $(a)\,(y)\equiv(b)$ has therefore a solution $(y)\neq(0)$ if $(a)\neq(0)$, $(b)\neq(0)$, and has a solution $(y)=(0)$, if $(b)=(0)$. Hence the classes (mod. $\bar{p}$) form a field of characteristic $\bar{p}$ if $\bar{p}$ is a prime number. On the other hand, if F is a field of characteristic $\bar{p}$, the elements $0, 1, \ldots, p-1$, from a subfield GF_p, and every subfield of F

---

[1] For the notation see (1, 10).

contains GF_p. Hence GF_p is the meet [1] of all subfields of F. As GF_p contains no other subfield, it is said to be a *Prime field* of characteristic p. Let F be a field of characteristic 0, then the elements $0, 1, 2, \ldots, -1, -2, -3, \ldots$ are all different and form a ring isomorphic to the ring of all integers, but not a field, *viz*. if n would be an integer, the equation $2n = 1$ has no solution.

If each element $a, b, c, \ldots$ of a ring R belongs to a field F, then [2/6]

$$ab = ba \quad \text{holds} \tag{1, 4m}$$

and
$$ab = 0\text{, if and only if } a = 0 \text{ or } b = 0\,, \tag{2, 7}$$

as these conditions hold for all elements of F. On the other hand, we will prove that if a ring satisfies the conditions (1, 4m) and (2, 7), it is a subring of a suitably chosen field.

Theorem. If the elements of a ring R satisfy the conditions (1, 4m) and 9. (2, 7), then R is a subring of a field.

Proof. We have to consider all pairs a, b of elements of R, where $b \neq 0$. The addition and the multiplication of these pairs should be defined by

$$\begin{aligned} a_1, b_1 + a_2, b_2 &= a_1 b_2 + a_2 b_1, b_1 b_2 \\ a_1, b_1 \;.\; a_2, b_2 &= a_1 a_2, b_1 b_2 \end{aligned} \tag{2, 8}$$

By this definition commutative and associative laws of addition and of multiplication and also the distributive law are satisfied (the reader may verify it). As b_1 and b_2 are different from 0, $b_1 b_2 \neq 0$. The pairs form therefore a system Σ of double composition. The system I of the pairs $0, b$ has the property that the sums of the elements of I and also the products of the elements of I with the elements of Σ are contained in I. From [2/3] it follows therefore that I generates a partition of Σ into classes, and the representation of a, b by its class a/b is a homomorphism of Σ. Let $\overline{Q}_R$ be the system of the classes a/b.* In order to prove that $\overline{Q}_R$ is a field we should only prove that that there exist x_1/x_2 and y_1/y_2 satisfying the conditions

$$\begin{aligned} x_1/x_2 + a_1/b_1 &= a_2/b_2 \\ y_1/y_2 \cdot a_0/b_0 &= a_3/b_3 \end{aligned}$$

a_0 being different from 0. These conditions are satisfied by

$$x_1 = a_2 b_1 - a_1 b_2,\quad x_2 = b_1 b_2 \neq 0.\ y_1 = a_3 b_0,\ y_2 = b_3 a_0 \neq 0\,.$$

Hence $\overline{Q}_R$ is a field. The elements $a/1$ form a subring of $\overline{Q}_R$ isomorphic to R. If we replace therefore these elements in $\overline{Q}_R$ by the corresponding elements of R, we will get a field Q_R isomorphic to $\overline{Q}_R$ and containing R as a subring.

---

[1] The elements common to the sets A, B,... form a set which is called the "meet" of A, B,... The elements contained in any of the sets A, B,... form a set which is called the "join" of A, B, ...

Theorem. Every subfield of F containing the subring R has a subfield $F(R)$ isomorphic to Q_R. $F(R)$ is composed of the quotients of the elements of R, and is the meet of all subfields of F containing R.

Proof. As $b/1 \cdot a/b = a/1$ holds, every element of Q_R is the quotient of two elements of R. The pairs of elements a, b of R, for which $bx = a$ holds, can be considered as a class representing the element x of F. This partition of the pairs into classes is the same as the partition by which the elements of $\overline{Q}_R$ have been defined ; also the addition and the multiplication of those quotients corresponds isomorphically to the addition and the multiplication of the elements of $\overline{Q}_R$ as these have been defined by (2, 8). Hence the system of those quotients is isomorphic to the field Q_R and is therefore a field $F(R)$ isomorphic to Q_R. Hence the theorem holds.

[2/7] Let F be a field of characteristic 0 ; the elements $0, \pm 1, \pm 2, \ldots$ form a subring R defining Q_R. R is isomorphic to the ring of the integers. In an arbitrary field of numbers the quotients of the integers form the field of the rational numbers; therefore Q_R is isomorphic to this field. As every subfield must contain the elements $0, \pm 1, \pm 2 \ldots$, the following theorem holds :

Theorem. If F is of characteristic 0, the meet of all subfields of F is a field Q_R isomorphic to the field of all rational numbers. In this isomorphism the elements m correspond to the integers m. Q_R is said to be the *Prime field* of F.

§ 3. POLYNOMIALS.

[3/1] Let S be a subring of a field,[1] and let x be different from all letters which have been used as symbols for elements of S. We will consider now new mathematical entities expressed by

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \Sigma\, a_i\, x^i. \tag{3. 1}$$

These new objects will be called *Polynomials*. a_i are elements of S, and are said to be the *Coefficients* of the polynomial. It should be noticed that these polynomials are other things than "functions"—although they have a certain connection with functions, which will be considered in [3/3]— x is not a symbol for a "variable" ! The polynomials are abstract elements defined by (3, 1) ; the calculation with these elements will be defined by the following definitions :

---

[1] These subrings will often be considered apart from its connection with a field of which they are subrings. In the German literature they are called "Integritätsbereiche." It would be convenient to have a special English expression for it. We will often use the abbreviation *s. r. o. f.*

The polynomials $\sum_{i=1}^{n} a_i x^i$ and $\sum_{i=1}^{m} a'_i x^i$ $m \geqq n$

are considered as *equal* if and only if $a_s = a'_s$, $s \leqq n$

$$a'_j = 0\ ,\ j > n. \tag{3, 2}$$

This definition of equality satisfies obviously the axioms (1,9) for equivalence.

$$\Sigma a_i x^i + \Sigma b_i x^i = \Sigma (a_i + b_i) x^i$$

$$\Sigma a_i x^i . \Sigma b_i x^i = \Sigma c_i x^i\ ,\ c_i = \Sigma a_j b_{i-j} \tag{3, 3}$$

The summation should be taken for all possible products $a_j\, b_{i-j}$.

The sums and products do not change, when a summand or a factor is replaced by a polynomial equal to it.

Let $a_s = 0$ for $s \geqq n$, and let either $n = 0$, or $a_{n-1} \neq 0$ then $n-1$ is said to be the *degree* of the polynomial $\Sigma a_i x^i$.

E.g., the polynomials whose coefficients are all equal to the nullelement of S have the degree -1, all other polynomials for which $0 = a_1 = a_2 = \ldots$ are of the degree 0, etc. There is a correspondence between the elements of S and the polynomials of degree < 1, where each element b of S corresponds to $b + 0x + 0x^2 + \ldots$. From (3, 3) it follows that this correspondence is an isomorphism. We therefore identify the polynomials of degree < 1 with the corresponding elements of S, and we shall then denote the set of the polynomials (3,1) by $S\,[x]$. So S becomes a subset of $S\,[x]$. The elements of $S\,[x]$ will often be denoted by

$f\,(x),\ \phi\,(x),\ \psi\,(x),\ \ldots$. The equation

$$f\,(x) = 0 \tag{3, 4}$$

means that $f\,(x)$ is the polynomial identified with the nullelement of S, *i.e.*, that $f\,(x)$ is a polynomial having no coefficient $\neq 0$ (polynomial of degree -1). It should be well understood that x is not an "unknown" and that therefore (3, 4) is not a "condition" that x should satisfy !

Sometimes this x will be called an *indefinite*.

If S contains a unitelement 1, there are in $S\,[x]$ elements $1x$, $1x^2$, ... $1x^n$ .... We may use for them the shorter notation x, x^2, ... x^n. From (3, 3) it follows that x^n is the n^{th} power of x, that $a_i x^i$ is the product of

R

a_i and x^i, and that $\Sigma\, a_i x^i$ is the sum of these products. We can therefore in this case generate every element of $S\,[x]$ from S and the indefinite x by repeated addition and multiplication If there is no unitelement in S, we may consider a field F of which S is a subring. F contains a unitelement, and $S\,[x]$ is a subset of $F\,[x]$, that can be generated from F and the indefinite x by addition and multiplication.

subring of a field.

[3/2] *Theorem.* $S\,[x]$ is an s. r. o. f.

Proof. The commutative and the associative laws, as well as the distributive law hold $\Sigma b_i x^i + \Sigma (a_i - b_i)\, x^i = \Sigma a_i x^i$; therefore the subtraction of polynomials can always be done, and $S\,[x]$ is a ring ; O is its nullelement. Let $\Sigma a_i x^i$ be of degree $n > -1$, and $\Sigma b_i x^i$ of degree $m > -1$, then $\Sigma a_i x^i\, \Sigma b_i x^i \ddagger O$, *viz.* $\Sigma a_{m+n-1} b_1 = a_n b_m \ddagger O$. Therefore a product of two polynomials $\ddagger O$ is different from O ; as it has been shown in [2/6], $S\,[x]$ is a subring of a field

As S was supposed to be an arbitrary s. r. o. f. we can repeat the procedure by taking for S the s. r. o f. $T = S\,[x]$. Then $T[y]$ is an s. r. o. f. Its elements are of the form $\Sigma a_{ik} x^i y^k$, a_{ik} being elements of S. We get the same elements by considering the polynomials in the indefinite x with coefficients from $S\,[y]$. Hence we denote $T\,[y]$ by

$$T\,[y] = S\,[x, y] = S\,[y, x] \qquad (3,\ 5)$$

and the polynomials of this s. r. o. f. are said to be *Polynomials in x and y.* By further repetition of this procedure we may get rings of polynomials in 3, 4, ... , n indefinites $S\,[x, y, \ldots, w]$. and each of these rings is a subring of a field.

Exercises. 1. Let $(a_0, a_1, a_2, \ldots)$ be an ordered enumerable infinite set of elements only a finite number of these elements being $\ddagger O$; by defining the addition and the multiplication for these sets in a suitable manner we may get a system isomorphic to $S\,[x]$.

2. If in the definition (3, 2) of the equality of polynomials, the 2nd condition be omitted, the system defined in this manner would not become a ring, still we can get $S\,[x]$ from it by a suitable homomorphism.

[3/3] Let S and therefore $S\,[x]$, be an s. r. o. f., and let Σ be a system of double composition containing S. To every polynomial

$$f\,(x) = a_0 + a_1 x + \ldots + a_n x^n \qquad (3,\ 6)$$

BCU 1740

28

E. Each polynomial can be expressed by $f(x)=a\phi(x)$, where $\phi(x)$ is primitive ; in two representations of this kind, the corresponding factors are associated.

Proof. If a is the highest common factor of the co-efficients of $f(x)$, then $f(x)=a\phi(x)$, and no prime element of S is a common factor of the co-efficients of $\phi(x)$; hence $\phi(x)$ is primitive. If $f(x)=a_1\phi_1(x)$ and $\phi_1(x)$ is primitive, then a_1 is the h.c.f. of the coefficients of $f(x)$; hence a_1 is associated to a, and therefore $\phi_1(x)$ is associated to $\phi(x)$.

Proof of 2. If $f(x)$ is an arbitrary element of $S[x]$, then $f(x)=a\phi(x)$, where $\phi(x)$ is primitive. Let $N(\phi(x))$ be the degree of $\phi(x)$, then the conditions of [4/4] are satisfied; hence the primitive polynomials of $S[x]$ are factorisable, and as the elements a of S are also factorisable, $f(x)$ is factorisable. Let there be two different factorisations of $f(x)$, and let a and a_1 be the products of those factors, which are elements of S. $f(x)=a\phi(x)$ $=a_1\phi_1(x)$; then $\phi(x)$ and $\phi_1(x)$ are primitive polynomials. Hence a is associated to a_1 and $\phi(x)$ is associated to $\phi_1(x)$. As a is uniquely factorisable, we have only to prove, that any primitive polynomial is uniquely factorisable. This theorem is true for $N(\phi(x))=1$. Let it be true for $N<r$, then it holds also for the corresponding non-primitive polynomials. Let

$$\begin{aligned}\chi(x)=\phi.\phi_1.\ \ldots\ \phi_r&=\psi.\psi_1.\ \ldots\ \psi_s\\ =\phi.\Phi\qquad&=\psi.\Psi\end{aligned}$$

be two different factorisations of a polynomial $\chi(x)$, $N\chi(x)=r$. As $\chi(x):\phi$ cannot be factorised in two different ways, the factors of the first factorisation are all different from the factors of the second one. Let

$$\begin{aligned}\phi(x)&=a_0+\ldots+a_nx^n \qquad m\leqq n,\ a_n\neq 0,\ b_m\neq 0\\ \psi(x)&=b_0+\ldots+b_mx^m\\ \omega(x)&=b_m\phi-a_nx^{n-m}\psi\\ \Omega&=\omega\Phi\end{aligned}$$

is of degree$<r$ and therefore uniquely factorisable, but $\Omega=b_m\chi(x)-a_nx^{n-m}\psi.\Phi=\psi(b_m\Psi-a_nx^{n-m}\Phi)$.

As Φ is not divisible by ψ, and ψ is irreducible, ω is divisible by ψ, hence $b_m\phi$ is divisible by ψ; from B it follows that ϕ is divisible by ψ, contrary to the supposition. Hence the theorem holds.

As $S[x]$ is uniquely factorisable if S, $S[x, y]$, $S[x, y, z]$, ...,$S[x,...,w]$ are also uniquely factorisable. Another consequence is, that the classes of residues of an irreducible polynomial in $S[x]$ form an s.r.o.f., but the factorisation in this ring ought not to be unique. It is one of the fundamental problems of the theory of the algebraic numbers to investigate the

104, 707

factorisation in rings of this kind. In §11 an example of such an s.r.o.f. will be considered; in that case the factorisation is unique.

[4/7] Let F be a field; and therefore be uniquely factorisable; hence (see [4/6]) the factorisation in $F[x]$ is unique.

Theorem. Let $\phi(x)=a_0+a_1x+\ldots+a_nx^n$, $w(x)=b_0+b_1x+\ldots+b_mx^m$ be polynomials of $F[x]$, $a_n \neq 0 \neq b_m$, $n \geq m$, then there is a polynomial $\chi(x)$ in $F[x]$ so that $\phi(x)-\chi(x)w(x)$ is of degree $<m$.

Proof. We construct a sequence of polynomials $\phi_1(x),\ldots,\phi_i(x)=\sum\limits_{s=0} a^i_s x^s,\ldots$ where $a^i_{n_i} \neq 0$ for every i, by the equations

$$\phi(x) - \frac{b_m}{a_n} x^{n-m} w(x) = \phi_1(x)$$

$$\phi_i(x) - \frac{b_m}{a_{n_i}} x^{n_i-m} w(x) = \phi_{i+1}(x)$$

The degrees of $\phi_1(x), \ldots, \phi_i(x), \ldots$ are decreasing, and the construction of the sequence can be continued till the degree becomes $<$m. Let $\psi_q(x)$ be the polynomial of the sequence having a degree $<$m, then $\phi_q(x) = \phi(x) - \chi(x)w(x)$. Hence the theorem holds.

The method for getting $\phi_q(x)$ by a finite number of steps is well known in elementary algebra as the *Algorithmus of division*. $\phi_q(x) = 0$ if and only if $w(x)$ is a factor of $\phi(x)$.

Theorem. The h.c.f. $(\phi(x), \psi(x))$ can be expressed by

$$(\phi(x), \psi(x)) = \phi(x)u(x)+\psi(x)v(x).$$

Proof. The theorem is trivial if one of the polynomials is the polynomial 0. Let $\phi(x)$ be $\neq 0$; we define N by $N(\phi(x))=1+\text{degree}\,(\phi(x))$. From the previous theorem, it follows that the suppositions of [4/5] are satisfied, and therefore the theorem holds.

Corollary. If each common factor of $\phi(x)$ and $\psi(x)$ is an element of F, every element $f(x)$ of $F[x]$ can be expressed by $f(x) = \phi(x)\psi_1(x)+\psi(x)\psi_1(x)$.

Proof. As $(\phi(x), \psi(x))=1$, there is an equation $1=\phi(x)u(x)+\psi(x)v(x)$. By multiplying this equation by $f(x)$, and taking $u(x)f(x)=\phi_1(x)$, $v(x)f(x)=\psi_1(x)$ we get the proposition.

Theorem. If $\phi(x)$ is irreducible in $F[x]$, the classes of residues of $\phi(x)$ in $F[x]$ form a field.

Proof. As it has been shown in the first theorem of [4/6], the classes form an s.r.o.f. $(\psi(x)) \neq (0)$, if and only if $\psi(x)$ is not divisible by $\phi(x)$.

In this case an arbitrary $f(x)$ can be represented by

$$f(x) = \phi(x)\,\phi_1(x) + \psi(x)\psi_1(x)$$

hence[1] $(f(x)) = (0) + (\psi(x))\,(\psi_1(x))$. An arbitrary $(f(x))$ can therefore be divided by every class $\neq (0)$. Hence the classes form a field.

Exercises. 1. Let S be an s.r.o.f. in which the factorisation is unique, let $\phi(x)$ and $w(x)$ be polynomials of $S[x]$ of degree n and m, $n \geq m$, $w(x)$ primitive. Prove that there is $\overline{w}(x)$ of degree $>$m, $\overline{w}(x) = a\,\phi(x) - \chi(x)w'(x)$, and $\overline{w}(x) = 0$ only if $w(x)$ is a factor of $\phi(x)$.

2. Let I be the ring of the integers. Prove that $((x^2+1), (x^2-1))$ cannot be represented by $u(x)(x^2+1) + v(x)(x^2-1)$, $u(x)$, $v(x)$ being polynomials of $I[x]$.

§ 5. EXTENSION OF A FIELD.

Let K be a subfield of an arbitrary field P, let $K[x]$ be the ring of [5/1] the polynomials in an indefinite x (see [3/1]) with co-efficients from K. As this ring is an s.r.o.f. (see [3/2]), it defines a quotient-field, that will be denoted by $K(x)$. The ring of the polynomials of n indefinites $x_1, \ldots, x_n$ will be denoted by

$$K[x_1, \ldots, x_n] \tag{5, 1}$$

and its quotient field by

$$K(x_1, \ldots, x_n) \tag{5, 2}$$

Let

$$a_1, \ldots, a_n \tag{5, 3}$$

be arbitrary, but fixed elements of P. To every polynomial $f(x_1, \ldots, x_n)$ of $K[x_1, \ldots, x_n]$, there is an integral function (see [3/3]), having an uniquely defined value $f(a_1, \ldots, a_n)$. These values, for arbitrary but fixed $a_1, \ldots, a_n$, form a ring

$$K[a_1, \ldots, a_n] \tag{5, 4}$$

Every ring containing K and (5, 3) contains each element of (5, 4); hence (5, 4) is the meet[2] of all the rings containing K and (5, 3). As

---

[1] We use the notation (1, 10).

[2] See the footnote, p. 13.

$K[a_1,\dots,a_n] \subseteq P$, (5, 4) is an s.r.o.f. The quotients $\beta_1 : \beta_2$ $(\beta_2 \neq 0)$ of the elements of (5, 4) form therefore (see [2/6]) a field

$$K(a_1,\dots,a_n) \qquad (5,\ 5)$$

The meet of all the rings containing K, and $a_1,\dots a_n$ is the set of all elements we get by repeated addition, subtraction and multiplication of the elements of K and $a_1,\dots,a_n$. In the same manner we get the ring (5, 1) as the set of all the polynomials, generated by addition, subtraction and multiplication of $x_1,\dots,x_n$ with elements of K. Hence, if $x_1\dots,x_n$ are elements of P, the notation $K[x_1,\dots,x_n]$, as it is defined by (5, 5), means the same as (5, 1). On considering the division (by elements $\neq 0$) besides addition, subtraction and multiplication we may get in the same manner, that if $x_1,\dots,x_n$ are elements of P, (5, 5) gives for $a_i = x_i$ the field (5, 2).

Each element of $K(a_1,\dots,a_n)$ can be written by

$$f(a_1,\dots,a_n) : \phi(a_1,\dots,a_n) ; \qquad (5,\ 6)$$

on the other hand (5, 6) denotes an element of (5, 5) if and only if the notation has any sense, *i.e.*, if

$$\phi(a_1,\dots,a_n) \neq 0 \qquad (5,\ 6_0)$$

$K[a_1,\dots a_n]$ is homomorphic to $K[x_1,\dots,x_n]$, but $K(a_1,\dots,a_n)$ is in general not homomorphic to $K(x_1,\dots,x_n)$.

Theorem. If $K[x_1,\dots,x_n]$ and $K[a_1,\dots,a_n]$ are isomorphic, $K(x_1,\dots,x_n)$ and $K(a_1,\dots,a_n)$ are also isomorphic ; if $K[x_1,\dots,x_n]$ and $K[a_1,\dots,a_n]$ are not isomorphic, $K(x_1,\dots,x_n)$ and $K(a_1,\dots,a_n)$ are not homomorphic.

Proof. If $K[x_1,\dots,x_n]$ and $K[a_1,\dots,a_n]$ are isomorphic, there is a (1, 1) correspondence between the polynomials $f(x_1,\dots,x_n)$ and the values $f(a_1\dots,a_n)$; hence $f(a_1,\dots,a_n) = 0$ holds if and only if f is the polynomial 0. To every element $f(x_1,\dots,x_n) : \phi(x_1,\dots,x_n)$ of $K[x_1\dots x_n]$ there corresponds therefore an element $f(a_1\dots,a_n) : \phi(a_1\dots a_n)$. Sums differences, products and quotients of corresponding elements correspond; hence the correspondence is a homomorphism. The value 0 is the image of no other element of $K(x_1,\dots,x_n)$, than of the polynomial 0; from [2/2] it follows that the homomorphism is an isomorphism. If

$K[\alpha_1,\ldots,\alpha_n]$ is homomorphic, but not isomorphic to $K[x_1,\ldots,x_n]$, to every element of $K[\alpha_1,\ldots,\alpha_n]$ there corresponds more than one polynomial; *e.g.*, to the value 0 there must correspond a polynomial ϕ different from the polynomial 0. Hence $\phi(\alpha_1,\ldots,\alpha_n) = 0$. There is therefore no value corresponding to the quotients $f(x_1,\ldots,x_n) : \phi(x_1,\ldots,x_n)$.

Theorem. If $K[\alpha]$ and $K[x]$ are not isomorphic, $K[\alpha]$ is isomorphic to the field of the classes of residues of an irreducible polynomial $f(x)$ in $K[x]$, and $K[\alpha]$ is identical with $K(\alpha)$. 9 [5/2]

Proof. As $K[\alpha]$ is homomorphic, but not isomorphic to $K[x]$, there is more than one polynomial which corresponds to 0. These form a ring R containing 0 and polynomials of degree >0. In R let n be the minimum positive degree and $f(x)$ be a polynomial of degree n. The classes of residues[1] of R in $K[x]$ form a ring isomorphic to $K[\alpha]$. We will prove that these classes are identical with the classes of residues of $f(x)$ in $K[x]$. Polynomials from the same class of $f(x)$ belong also to the same class of R. In every class of $f(x)$ there are polynomials of degree $>$n. Therefore if different classes of $f(x)$ are contained in one class of R, then there exist two polynomials belonging to the same class, such that their difference is a polynomial of degree m, $-1 \angle m \angle n$. This polynomial should belong to R in contradiction to the definition of n. Hence R is the ring of the polynomials divisible by $f(x)$. If $f(x)$ would be reducible, $f(x) = f_1(x)f_2(x)$, both the factors being of positive degree, these degrees must be $<$n; hence $f_1(\alpha) \ddagger 0$, $f_2(\alpha) \ddagger 0$, contrary to $0 = f(\alpha) = f_1(\alpha)f_2(\alpha)$. In [4/7] it has been proved that the classes of residues of an irreducible polynomial form a field. Hence $K[\alpha]$ is a field, and as $K(\alpha)$ is the meet of all fields containing $K[\alpha]$, $K[\alpha]$ is identical with $K(\alpha)$.

$K[\alpha_1,\ldots,\alpha_n]$ is called the *extension* of K by $\alpha_1,\ldots,\alpha_n$. There are two different kinds of extensions of a field by one element α. If the values of $\phi(\alpha)$ for the different polynomials ϕ of $K[x]$ are all different, $K(\alpha)$ is said to be a *transcendental extension*, and α is said to be transcendental to K. If those values are not all different, the extension is said to be *algebraic*, and α is algebraic to K. By using these notions we get the following

---

[1] See [2/3].

Corollary. If α is algebraic to K, K(α) is equal to K $[\alpha]$ and is isomorphic to the classes of residues of an irreducible polynomial $f(x)$ and $f(\alpha)=0$.

Proof. As α is algebraic to K, K $[\alpha]$ and K $[x]$ are not isomorphic; hence the proposition follows directly from the last theorem.

Theorem. If α is transcendental to K and x is an indefinite not belonging to K, then K (α) is isomorphic to K (x), and therefore all transcendental extensions of K by one element are isomorphic.

Proof. As all values $\phi(\alpha)$ are different, the homomorphism $\phi(x) \rightarrow \phi(\alpha)$ is an isomorphism, and therefore the theorem follows directly from [5/2].

[5/3] *Fundamental theorem of general algebra.* To every polynomial $\phi(x)$ of positive degree in K $[x]$ there is an algebraic extension $\mathrm{P} = \mathrm{K}(\alpha)$ such that $\phi(\alpha) = 0$.

Proof. Let $f(x)$ be an irreducible factor of $\phi(x)$. The classes of residues of $f(x)$ form a field P (see [4/7]). Let α be the element of P, that corresponds to the polynomial x of K $[x]$, then $f(\alpha) = 0$, and therefore $\phi(\alpha) = 0$. The elements of P correspond to polynomials in x, and are therefore integral functions of α with co-efficients from K. Every field containing K and α must therefore contain P. Hence $\mathrm{P} = \mathrm{K}(\alpha)$.

On dividing $f(x)$ by $x - \alpha$ we get $f(x) = (x - \alpha)\ \psi(x) + \alpha'$. As $f(\alpha) = 0$, $\alpha' = 0$. I. e., $f(x)$ is divisible by $x - \alpha$.

Theorem. Every polynomial P (x) of positive degree in K $[x]$ becomes in a suitable extension of K a product $a\Pi(x-\alpha_i)$ of linear polynomials.

Proof. From the fundamental theorem we know that their exists an extension P_1 of K, containing an element α_1 for which $\phi(\alpha_1) = 0$, and therefore $\phi(x) = (x - \alpha_1)\psi_1(x)$. The degree of ψ_1 is less than the degree of ϕ. In a suitable extension P_2 of P_1 ψ_1 becomes divisible by $x - \alpha_2$ and therefore $\psi(x) = (x - \alpha_1)(x - \alpha_2)\psi_2(x)$. By repetition of this procedure we will get after a finite number of steps a decomposition of $\phi(x)$ into linear factors. The fundamental theorem of general algebra is in a certain sense a generalisation of another theorem that has generally been called the "fundamental theorem of algebra." When we will have to deal with that theorem in [13/9], it will be called the fundamental theorem of classical algebra in order to avoid any confusion.

In Part I we started from the problem:

Given arbitrary numbers $a_0, a_1, \dots, a_n, \dots \dots, k_n$ called the co-efficients, we are required to find out n numbers $x_1, \dots, x_n$ satisfying the m conditions $\Sigma a_i x_i = a_0, \dots, \Sigma k_i x_i = k_0$. It is necessary to note that the solutions of this problem and the theorems connected with it are of more general character than those given there. [5/4]

If in Part I, formula (1), (2), (2H), (3), (4) (6), (7), (10), (11), (14), (15), the notion of "arbitrary number" is replaced by "arbitrary element of an arbitrary and fixed field K,*" every proposition of pp. 1-13 holds*

The *proof* of each proposition of these pages will not be changed, if in these propositions and in the definitions previous to them the replacement mentioned above has been effected. The reader may go again through those pages. The considerations given there will not be repeated here. About the other sections of Part I it may be mentioned that § 9 does not hold for an arbitrary field unless the definitions of "scalar product" and of "orthogonality" have been modified (that can be done, but will not be done here) All other considerations of Part I hold without any change for arbitrary fields of characteristic $\neq 2$. For fields of characteristic 2 the proofs of Theorem VIII and of Theorem X have to be modified. In the proof of Th. VIII the number $\frac{1}{2}$ has been used, which is not an element of fields of characteristic 2. In the proof of Th. X it has been argued that from $D = -D$ it follows that $D = 0$. This is true if and only if D is an element of a field K of characteristic $\neq 2$, but in a field of characteristic 2 every element D is equal to $-D$. The reader may make the necessary modifications of those proofs as an *exercise*. In the text only the generalisation of pp. 1-13 will be used.

Let K be a field and M be a modul. If the multiplication of the elements of K with the elements of M is defined in such a manner, that the multiplication of an arbitrary element of K with the elements of M is a distributive operation in M, then M is said to be a *modul over* K. The elements $a_1, \dots, a_m$ are said to be *independent*, if $c_1 a_1 + \dots + c_m a_m \neq 0$, for every system $(c_1, \dots, c_m) \neq (0, \dots, 0)$ of elements of K. If there is a maximum number r of independent elements in M, r is said to be the *rank* of M *over* K.

Let r be the rank of M over K and $a_1, \dots, a_r$ be independent elements of M, then these elements form a *Basis* of M, and every element α of M can be expressed in one and only one manner by

$$\alpha = c_1\alpha_1 + \dots + c_r\alpha_r . \qquad (5, 7)$$

There is therefore an (1, 1)-correspondence between the elements (5, 7) and r-vectors $(c_1, \dots, c_r)$, and by this correspondence the sum of two elements corresponds to the sum of the corresponding r-vectors. M can therefore be considered as a *vectorspace over* K, *i.e.* a vectorspace as it has been defined in Part I, p. 6, but the co-ordinates being elements of K, where K is an arbitrary field and may therefore be different from the field of the real numbers. A basis of the modul M is at the same time a basis of the vectorspace M. From Part I, p. 7, we get therefore immediately the following

Theorem. Every basis of M has the same number of elements

$$r = [M : \mathrm{K}] \qquad (5, 8)$$

and if M, M_1 are different moduls over K, so that every element of M belongs to M_1, then

$$[M_1 : \mathrm{K}] > [M : \mathrm{K}] \qquad (5, 9)$$

[5/5] If the modul F over K is a field containing the unit element of K, then it contains every element of K, *i.e.*, K is a subfield of F. In this case F is said to be a *field over* K, and if especially there is a finite number $[F : \mathrm{K}]$, F is said to be *finite over* K.

Theorem. If K_1 is finite over K, and K_2 is finite over K_1, than K_2 is finite over K, and

$$[\mathrm{K}_2 : \mathrm{K}] = [\mathrm{K}_2 : \mathrm{K}_1] : [\mathrm{K}_1 : \mathrm{K}] \qquad (5, 10)$$

holds.

Proof. Let $\alpha_1, \dots, \alpha_r$ be a basis of K_1 over K, and $\beta_1, \dots, \beta_s$ be a basis of K_2 over K_1, then every element of K_2 is uniquely given by

$$d = \sum_{i=1}^{r} c_i\alpha_i , \text{ and every element of } \mathrm{K}_2 \text{ by } \sum_{j=1}^{s} d_j\,\beta_j = \sum c_{i,j}\,\alpha_i\,\beta_j ,$$

c_i and $c_{i,j}$ being elements of K. In order to prove that the r.s elements $\alpha_i\beta_j$ form a basis of K_2 over K, we have only to prove that they are independent over K. Let $0 = \Sigma g_{i,j}\,\alpha_i\beta_j = \Sigma\,\beta_j\,\Sigma g_{i,j}\,\alpha_i$. As β_j are independent in K_2 over K_1, for every j $\Sigma\,g_{1,.}\,\alpha_i \neq 0$. As α_i are independent over K, each $g_{i,j}$ has to be equal to 0. Hence the r.s elements $\alpha_i\text{-}\beta_j$ form a basis of K_2, and the theorem holds.

Theorem. If K is a subfield of K_1, K_1 is a subfield of K_2, and K_2 is finite over K_1, then K_2 is finite over K_1, and (5, 10) holds.

Proof. As every element of K_1 belongs to K_2, there cannot be more than $[K_2 : K]$ independent elements of K_1 over K; hence K_1 is finite over K. For the same reason K_2 must be finite over K_1. Hence the suppositions of the preceding theorem are satisfied, and (5, 10) therefore holds.

Theorem. If K_1 is finite over K, every element of K_1 is algebraic to K. [5/6]

Proof. Let $[K_1 : K] = r$, and α be an arbitrary element of K_1; then the r + 1 elements $1, \alpha, \ldots, \alpha^r$ are not independent over K, and therefore an equation $\Sigma\,a_i\,\alpha^i = 0$ holds, where a_i are elements of K, and not all of them are equal to zero.

omit

Theorem. Let $f(x)$ be an irreducible polynomial of $K[x]$ and of order n; let $f(\alpha) = 0$ and β be an arbitrary element of $K(\alpha)$, then $K(\alpha)$ is finite over K, and $[K(\beta) : K] = n$. β is a root of an irreducible polynomial belonging to $K[x]$ of order $m > n$; $[K(\beta) : K] = m$. α is a root of an irreducible polynomial with co-efficients from $K(\beta)$ of order n : m, and m is therefore a factor of n.

Proof. The elements $1, \alpha, \ldots, \alpha^{n-1}$ are independent over K, as α is not a root of a polynomial belonging to $K[x]$ and of positive degree less than n. On the other hand every element of $K(\alpha)$ can be expressed by $\sum_{i=0}^{n-1} c_i\,\alpha_i$. Hence $1, \alpha, \ldots, \alpha^{n-1}$ form a basis of $K(\alpha)$, and $[K(\alpha) : K] = n$.

Therefore every element β of $K(\alpha)$ is algebraic to K. On making the same consideration for β that has just been done for α, we find out that $[K(\beta) : K] = m$.

Let $K(\beta) = M$, then $K(\alpha) = M(\alpha)$. $M(\alpha)$ is finite over M, and from (5.10) it follows that $[M(\alpha) : M] = n : m$; on the other hand this number is equal to the degree of an irreducible polynomial belonging to $M[x]$, of which α is a root.

[5/7] Let $f(x) = \Sigma c_i x^i$ be a polynomial of $K[x]$. Then for the derivate $f'(x) = \Sigma i c_i x^{i-1}$ holds. Therefore the derivate is the polynomial 0, if and only if $0 = c_1' = 2c_2 = nc_n$ holds, *i. e.*, if all co-efficients are equal to zero except atmost some of those whose index is a multiple of the characteristic of K. If the characteristic is 0, the degree of $f(x)$ is less than one; if the characteristic is a prime number p, $f(x)$ must be a polynomial of x^p. Hence the following theorem holds:

Theorem. Let $f(x)$ be a polynomial of positive degree, then $f'(x) = 0$, if and only if the characteristic of the field of the co-efficients of f is a prime number p, and $f(x) = \phi(x^p)$.

In a suitable field $f(x)$ can be represented as a product.

$f(x) = a(x - \alpha_1). \dots . (x - \alpha_n)$. Hence

$$f'(x) = a(x - \alpha_2). \dots , (x - \alpha_n) + \dots + a(x - \alpha_1). \dots , (x - \alpha_{n-1})$$

$$= \Sigma f(x) : (x - \alpha_i). \qquad (5, 11)$$

The h.c.f. $(f(x), f'(x)) = R(x)$ is a polynomial of $K[x]$. If $f'(x) = 0$, $f(x) = R(x)$. In every other case the degree of $R(x)$ is less than the degree of $f'x)$. As the roots of $R(x)$ are roots of $f(x)$.

$$R(x) = (x - \alpha_{i_1}). \dots .(x - \alpha_{i_m}) \quad .$$

$\alpha_{i_1}, \dots, \alpha_{i_m}$ being the common roots of $f(x)$ and $f'(x)$. From (5,11) it follows that $f'(\alpha_i) = a \prod_{i \neq k} (\alpha_i - \alpha_k)$. Hence α_i is a root of $R(x)$ if and only if two roots of $f(x)$ are equal, *i.e.* if $f(x)$ is divisible by $(x - \alpha_i)^2$. Therefore, if $f(x)$ is irreducible and of degree n, and $f'(x) \neq 0$, then $f(x)$ has n different roots. An irreducible polynomial of this kind is said to be *separable*. From [5/7] it follows

Theorem. An irreducible polynomial $f(x)$ of $K[x]$ is non-separable if and only if K is of characteristic p, and $f(x)$ is a polynomial in x^p, (Then $f'(x)=0$

Let $f(x)$ be irreducible and not separable, and let e be chosen in such a manner that $f(x) = \psi(x^{p^e})$, but $f(x)$ is not a polynomial in $x^{p^{e+1}}$.

Then $e > 0$. $\psi(y)$ is irreducible in K[y], *viz.*, $f(x)$ is irreducible in K[x] and it is a separable polynomial of K[y], *viz.*, if it would not be separable, it should be $\psi(y) = \chi(y^p)$ and therefore $f(x) = \chi(x^{p^{e+1}})$.

We will consider an arbitrary extension P of the field K in which the polynomial ψ is a product of linear factors

$\psi(y) = (y - \beta_1) \ldots\ldots, (y - \beta_m)$, $\beta_1, \ldots, \beta_m$ being different ; hence $f(x) = (x^{p^e} - \beta_1). \ldots . (x^{p^e} - \beta_m)$.

In a suitable extension of P there are solutions γ of $x^{p^e} - \beta_i = 0$.

As $(x - \gamma)^{p^e} = x^{p^e} + pF(x,\gamma) - \gamma^{p^e} = x^{p^e} - \gamma^{p^e}$, γ is a root of $f(x)$, and

$$f(x) = a\Pi(x - \alpha_1)^{p^e} \tag{5,12}$$

holds, where all α_i are different, *viz.*, $\alpha_i^{p^e} = \beta_i$. By these considerations the case of the not separable polynomials is reduced to the case of the separable polynomials.

[5/8] Let K be an arbitrary field, $\Lambda = K(\alpha_1, \ldots, \alpha_m)$ an extension of K and $f(x_1, \ldots, x_m)$ an arbitrary polynomial of K $[x_1, \ldots, x_m]$; then $f(\alpha_1, \ldots, \alpha_m)$ is an element of Λ, and all these elements form a subring R of Λ. The quotient-field of R contains K $(\alpha_1, \ldots, \alpha_m)$ and therefore every element of Λ ; on the other hand each of its elements is contained in Λ. Hence it is identical with Λ. *i.e.*

Theorem. Every element of $K(\alpha_1, \ldots, \alpha_m)$ is the quotient of two elements of the type $f(\alpha_1, \ldots, \alpha_m)$, where f is a polynomial with co-efficients of K.

Theorem. If $\alpha_1, \ldots, \alpha_m$ are algebraic to K, every element of $K(\alpha_1, \ldots, \alpha_m)$ can be represented by $f(\alpha_1, \ldots, \alpha_m)$, where f is a polynomial with coefficients from K.

Proof. As it has been proved in the corollary of [5/2], $K[\alpha_1] = K(\alpha_1)$ holds. In order to prove the theorem by mathematical induction, we suppose that K $[\alpha_1, \ldots, \alpha_m] = K(\alpha_1, \ldots, \alpha_m) = K'$. As α_{q+1} is algebraic to K, it is also algebraic to K'; Hence $K'[\alpha_{q+1}] = K'(\alpha_{q+1}) = K(\alpha_1, \ldots, \alpha_{q+1})$.

By mathematical induction $K[\alpha_1, \ldots, \alpha_m] = K(\alpha_1, \ldots, \alpha_m)$ follows.

Hence the theorem holds.

[5/9] There are two methods of making an algebraic extension of a field K. If K is a subfield of Ω and $\alpha_1, \ldots, \alpha_n$ are elements of Ω algebraic to K, then $K(\alpha_1, \ldots, \alpha_n)$ is a uniquely defined algebraic extension of K. On the other hand, if $f(x)$ is an irreducible polynomial of $K[x]$, we can find out fields over K in which $f(x)$ has a root, and if α is such a root, there is an extension $K(\alpha)$. This extension has not been uniquely defined by K and $f(x)$, but it follows from the corollary of [5/2], that the extensions $K(\alpha)$ are all isomorphic. If $f(x)$ is reducible, $f(x) = \psi_1(x) \ldots . \psi_r(x)$, we can extend K by a root of $\psi_1(x)$, or of $\psi_2(x), \ldots,$ or of $\psi_r(x)$, but these extensions are not necessarily isomorphic. This procedure may be repeated. If $f_1(x), f_2(x), \ldots, f_n(x)$ are polynomials of $K[x]$, then there exist extensions $K(\alpha_1, \ldots \alpha_n)$, such that α_i is a root of $f_i(x)$. These extensions are not necessarily isomorphic, even in the case that the polynomials are all irreducible in $K[x]$, *viz*. if α is a root of $f_1(x)$, the polynomial of $f_2(x)$ may be irreducible in $K(\alpha)$.

In the following *examples* K denotes the field of the rational numbers.

1. $f_1(x) = x^2 - 2, f_2(x) = x^4 - 2$

$$\alpha^2 = 2, f_2(x) = (x^2 - \alpha)(x^2 + \alpha) \qquad K(\alpha) = K_1$$

$$\beta^2 = \alpha, \beta'^2 = -\alpha; K_1(\beta) = K(\beta), K_1(\beta') = K(\beta')$$

Hence $K(\alpha, \beta)$ and $K(\alpha, \beta')$ are isomorphic. It may be mentioned that these two isomorphic fields of numbers are different fields, the first is a field of real numbers and the second contains complex numbers.

2. $f_1(x) = x^3 - 2, f_2(x) = x^6 - 2$

$$\alpha^3 = 2 \quad f_2(x) = (x^2 - \alpha)(x^4 + \alpha x^2 + \alpha^2) \quad K(\alpha) = K_1$$

$$\beta^2 = \alpha \;, \beta'^4 + \alpha\beta'^2 + \alpha^2 = 0. \quad K_1(\beta) = K_2 \quad , \quad K_1(\beta') = K_3$$

If we would show that the two factors of $f_2(x)$ are irreducible, we would get the consequence : $[K_2 : K_1] = 2$, $[K_3 : K_1] = 4$, hence $[K_2 : K] = 6$, $K_3 : K = 12$. Hence the two extensions of the prime field K are not isomorphic. The same will be proved here without any reference to irreducibility.

$(2\beta'^2 + \alpha)^2 + \alpha^2 + \alpha^2 + \alpha^2 = 4(\beta'^4 + \alpha\beta'^2 + \alpha^2) = 0$, hence 0 is the sum of the squares of four numbers of K_3, which are surely not all equal to 0. K_3 can therefore not be isomorphic to a field containing real numbers only, *e.g.*, K_3 cannot be isomorphic to K_2.

§6. NORMAL EXTENSIONS OF A FIELD. [6/1]

In the last given example it has been shown that if $\alpha_1, \ldots, \alpha_n$ are defined only by the irreducible equations in K which they satisfy, the extensions $K(\alpha_1, \ldots, \alpha_n)$ are not necessarily isomorphic. However we have to consider now a very important special case in which such an isomorphism holds. For this purpose the following two definitions are helpful.

Let I be an isomorphism transforming a field K into a field Δ, by this isomorphism an arbitrarily chosen subring K' of K is transformed in a certain subring Δ', this transformation being an isomorphism I'. Then I is said to be an *Extension* of I'.

Let $f(x)$ be a polynomial of $K[x]$, then there exists an extension Δ of K, in which $f(x)$ becomes a product of linear factors. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in Δ, then $f(x)$ can be represented as a product of linear factors only in those subfields of Δ, which contain $K(\alpha_1, \ldots, \alpha_n)$. This field is therefore said to be a *smallest extension of* K *admitting the complete reduction of* $f(x)$.

Theorem. Let K and Λ be isomorphic, $f(x)$ and $\phi(x)$ be corresponding polynomials of $K[x]$ and $\Lambda[x]$, let K' be a smallest extension of K admitting the complete reduction of $f(x)$, and let Δ' be a smallest extension of Λ admitting the complete reduction of $\phi(x)$; then every isomorphism of K and Λ can be extended to an isomorphism of K' and Λ'.

Proof. The theorem holds obviously if $[K':K] = 1$ *viz.* in this case $K = K'$, and $\Lambda = \Lambda'$. To prove the theorem by mathematical induction, it will be supposed to hold for $[K':K] < m$. Let $[K':K] = m$, and $f_1(x)$ be an irreducible factor of $f(x)$ of degree $\nless 1$. Let $\phi_1(x)$ be the polynomial of $\Lambda[x]$ isomorphic to $f_1(x)$, let α be a root of $f_1(x)$ in K', and let β be a root of $\phi_1(x)$ in Λ'. We can extend the isomorphism of K and Λ to an isomorphism of the classes of residues of $f_1(x)$ in $K[x]$ and of $\phi_1(x)$ in $\Lambda[x]$, and therefore to an isomorphism of $K(\alpha)$ and $\Lambda(\beta)$. Every extension of $K(\alpha)$ admitting the complete reduction of $f(x)$ is an extension of K admitting the complete reduction of $f(x)$; hence K' is a smallest extension of $K(\alpha)$ admitting this reduction. For the same reason Λ' is a smallest extension of $\Lambda(\beta)$ admitting the complete reduction of $\psi(x)$. As $[K':K(\alpha)] < m$, the isomorphism of $K(\alpha)$ and $\Lambda(\beta)$ can be extended to an isomorphism of K'

and Λ', and as that isomorphism of $K(\alpha)$ and $\Lambda(\beta)$ is an extension of the given isomorphism of K and Λ, the theorem holds.

Corollary. The smallest extensions of K admitting the complete reduction of a polynomial $f(x)$ are isomorphic.

Proof. The representation of every element by itself is an isomorphism of K and $\Lambda = K$. By this isomorphism $f(x)$ corresponds to itself. So the corollary follows directly from the preceding theorem.

[6/2] Let $K \subset N$; if every irreducible polynomial of $K[x]$ has either no root in K, or it becomes a product of linear polynomials of $K[x]$, then K is said to be a *normal extension of* K.

omit *Theorem.* If K′ is a smallest extension of K admitting the complete reduction of an arbitrary polynomial $f(x)$ of $K[x]$, then K′ is a normal extension of K.

Proof. Let $\alpha_1,\ldots,\alpha_n$ be the roots of $f(x)$ in K′, let $g(x)$ be irreducible in K, let β and β' be roots of $g(x)$, β belonging to K′, and β' belonging to a suitable extension of K′. Therefore $K_1 = K(\beta)$ and $K_2 = K(\beta')$ are isomorphic, and there is an isomorphism of these fields by which every element of K corresponds to itself, and β corresponds to β'. From [6/2] it follows, that we can extend this isomorphism to an isomorphism of $K_2(\alpha_1,\ldots,\alpha_n)$ and $K_1(\alpha_1,\ldots,\alpha_n) = K(\alpha_1,\ldots,\alpha_n) = K'$. By this isomorphism every root of a polynomial with co-efficients from K will be represented by a root of the same polynomial; hence the elements α_i will only be interchanged. $\beta = F(\alpha_1,\ldots,\alpha_n)$, where the co-efficients of F are elements of K. Hence $\beta' = F(\alpha_{i_1},\ldots,\alpha_{i_n})$, and therefore β' belongs to K′. As β' is supposed to be an arbitrary root of $g(x)$, the theorem holds.

We will consider two different generalisations of this theorem.

Omit *Theorem.* Let $f_1(x), f_2(x),\ldots$ be polynomials of $K[x]$, finite or infinite in number; the smallest extension of K admitting the complete reduction of all these polynomials is a normal extension of K.

Proof. Let $F_m(x) = f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_m(x)$, and let K_m be the normal extension we get by extending K with the roots of $F_m(x)$; $m = 1, 2, \ldots\ldots$ The smallest extension of K admitting the complete reduction of all the $f_m(x)$ is the join[1] of the fields K_m. If therefore a polynomial $g(x)$ has a root in that extension, this root is an element of a suitable K_m, and as K_m is a normal extension of K, $g(x)$ becomes a product of linear polynomials in K_m and also in every extension of K_m. Hence the theorem holds.

---

[1] See the footnote, p. 13.

We will get another generalisation of the first theorem of [6/2] by considering now a polynomial $g(x)$ irreducible in $K[x]$ will be factorised in a field N normal over K. [6/3]

Let $\psi_1(x), \ldots, \psi_m(x)$ be irreducible factors of $g(x)$ in N. β_1 a root of $\psi_1(x)$ and β_2 a root of $\psi_2(x)$ in a suitable extension of N. The co-efficients of $\psi_1(x)$ are roots of polynomials $f_1(x), \ldots, f_r(x)$, irreducible in K. As N is normal over K, the roots of every $f_i(x)$ belong all to N. Let $\alpha_1, \ldots, \alpha_n$ be these roots ; then $K \subseteq K(\alpha_1, \ldots, \alpha_n) = \Lambda \subseteq N$. Λ is a finite extension of K and normal over K ; the factorization of $g(x)$ in Λ is the same as in N. As β_1 and β_2 are roots of $g(x)$, irreducible in K, the fields $K(\beta_1)$ and $K(\beta_2)$ are isomorphic, and there is an isomorphism by which β_1 is represented by β_2, and the elements of K do not change. Hence no $f_i(x)$ is changed by it. We can extend this isomorphism to an isomorphism of $K(\beta_1, \alpha_1, \ldots, \alpha_n) = \Lambda(\beta_1)$ and $K(\beta_2, \alpha_1, \ldots, \alpha_n) = \Lambda(\beta_2)$. As by this isomorphism $f_1(x)$ remains invariant, its roots are interchanged only ; hence an element of Λ is represented by an element of Λ. The polynomial $\psi_1(x)$ which is irreducible in Λ and which is a factor of the polynomial $g(x)$, irreducible in K must therefore be represented by a factor of $g(x)$ which is irreducible in Λ. As the root β_1 of $\psi_1(x)$ is represented by the root β_2 of $\psi_2(x)$, the image of $\psi_1(x)$ is $\psi_2(x)$, and as these two polynomials are arbitrary irreducible factors of $g(x)$, the following theorem holds :

Theorem. If $g(x)$ is irreducible in K, and N is normal over K, every irreducible factor of $g(x)$ in N can be transformed into every other by a suitable automorphism of a certain field over K ; hence these factors are all of the same degree.

If one of the irreducible factors is of degree 1, the others are linear too; so the first theorem of [6/2] is a special case of this theorem.

§7. CYCLOTOMIC EQUATIONS.

We have now to consider the equations [7/1]

$$x^n - 1 = 0 \tag{7, 1}$$

Its solutions in the field of the complex numbers are

$$e^{2\pi ik:n} = \cos 2\pi\frac{k}{n} + i \sin 2\pi\frac{k}{n} \tag{7, 2}$$

$k = 0, 1, \ldots, n-1$.

In the $z = x+iy$-plane the nutmbers (7, 2) are represented by points with the polar co-ordinates $r = 1$, $\psi_k = 2\pi\frac{k}{n}$. These points divide the circle with the radius 1 and the centre 0 in n equal arcs. The partition of a circle in n congruent arcs is therefore done by the solution of (7, 1). We shall consider the problem from a purely algebraic point of view.

Let $f(x) = x^n - 1$, hence $f'(x) = nx^{n-1}$. The h.c.f. $(f(x), f'(x))$ is 1 if n is not divisible by the characteristic of the field we consider, but if p is the characteristic, and $n = p^e n_0$, $e > 0$, and n_0 being not divisible by p, then $f'(x) = 0$, and $(f(x), f'(x)) = f(x)$.

In this case we take $y = x^{p^e}$, $\psi(y) = y^{n_0} - 1 = f(x)$.

$(\psi(x), \psi'(y)) = 1$, hence $\psi(y)$ has in a suitable extension of the field exactly n_0 different roots $y_1, \dots, y_{n_0}$

Let x_1 and x_2 be two roots of $x^{p^e} - y_1 = 0$, then $x_1^{p^e} - x_2^{p^e} = 0$.

From the Binomial theorem it follows that in a field of characteristic p the formula $(a+b)^p = a^p + b^p$ holds, and therefore $(a-b)^{p^e} = a^{p^e} + (-b)^{p^e}$ $= a^{p^e} - b^{p^e}$ for odd and for even values of p, as for $p = 2$ the addition and the subtraction of elements become identical. Therefore $(x_1 - x_2)^{p^e} = 0$; so to every root of $\psi(x)$ corresponds only one root of $f(x)$. Hence $f(x)$ has exactly n_0 different roots.

[7/2] We shall now suppose that n is not divisible by the characteristic of the field; this supposition includes the case when the characteristic is 0. Then $f(x)$ has n different roots in every extension of the field admitting the complete reduction of $f(x)$. The same holds for $x^h - 1 = 0$ when h is an arbitrary factor of n.

Let α and β be roots of $f(x)$, hence $\alpha^n = 1 = \beta^n$, then $(\alpha\beta)^n = 1$, $(\alpha : \beta)^n = 1$. The roots of $f(x)$ form a multiplicative abelian group Γ. Let r be the smallest positive integer for which $\alpha^r = 1$ holds, then r is said to be the *order* of α in Γ. As $\alpha^{sr+tn} = 1$ for every pair of integers s and t, it follows that r is a factor of n. On the other hand if r is a factor of n, then the roots of $x^r - 1$ are at the same time roots of $x^n - 1$. The elements of Γ of order n are called *primitive roots* of $f(x)$. $\phi(n)$ denotes the number of these primitive roots.

Let $n = q^k$, where q is a prime number, and $k > 0$. If α is a root of $f(x)$, but not primitive, $\alpha^{q^{k-1}} = 1$ as there are just q^{k-1} elements satisfying the condition, there are $q^k - q^{k-1}$ primitive roots. Hence

$$\phi(q^k) = q^k(1 - \frac{1}{q}). \qquad (7, 3)$$

Let $n = h.k$, $\phi(h, k) = 1$; let α be of order h and β be of order k ; the order of any power of α is a divisor of h, and the order of any power of β is a divisor of k. Hence $\alpha^r = \beta^s$ only if both sides of the equation are equal to 1, *i.e.* if r is a multiple of h, and s is a multiple of k. From $\alpha^r\beta^s = \alpha^{r'}\beta^{s'}$ it follows that $\alpha^{r-r'} = \beta^{s'-s}$, and therefore $r \equiv r'$ (mod. h), $s \equiv s'$ (mod. k). The $h.k$ products

$$\alpha^r\beta^s, \text{ where } r = 0, 1, \ldots, h-1 \text{ ; } s = 0, 1, \ldots, k-1 \qquad (7, 4)$$

are therefore all different, and as $f(x)$ has just $n = hk$ roots, each root can be represented by (7. 4). α^r is of order $< h$, if and only if $(r, h) > 1$.

The primitive roots of $x^h - 1$ are

$$\alpha, \alpha^{r_2}, \ldots, \alpha^{r_w}, (r_i, h) = 1, \phi(h) = w \text{ ; } \qquad (7, 5)$$

the primitive roots of $x^k - 1$ are

$$\beta, \beta^{s_2}, \ldots, \beta^{s_t}, (s_j, k) = 1, \phi(k) = t.$$

If $\alpha^{r'}$ and $\beta^{s'}$ are not both of order h and k respectively, the product is of order $< n$, and it is therefore not a primitive root.

If $(\alpha\beta)^u = (\alpha\beta)^v$, $\alpha^{u-v} = \beta^{v-u}$, therefore $u \equiv v$ (mod. h and mod. k). The powers $(\alpha\beta)^u$, $u = 0, 1, \ldots, n-1$ are therefore all different ; hence $\alpha\beta$ is a primitive root. The same hold if we replace α by another element of order h, and β by another element of order k. So it follows from (7, 5) that the primitive roots of $f(x)$ are

$$\alpha^{r_i}\beta^{s_j}, \ i = 1, \ldots, \phi(h) \text{ ; } j = 1, \ldots, \phi(k) \qquad (7, 6)$$

Hence $\phi(h.k) = \phi(h).\phi(k)$ holds for $(h,k) = 1$ (7, 7)

From (7, 3) and (7, 7) it follows by mathematical induction that :

If $n = q_1^{k_1}. \ldots . q_m^{k_m}$, and $q_1, \ldots, q_m$ are different prime numbers,

$$\phi(n) = n\Pi\left(1 - \frac{1}{q_i}\right) > 0. \qquad (7, 8)$$

If α is a primitive root, $n : (h, n)$ is the order of α^h, and therefore α^h is a primitive root if and only if $(h, n) = 1$. Hence the number of positive integers $< n$ and relatively prime to it is equal to $\phi(n)$.

The essence of these considerations is given by the following theorem.

Theorem. If x^n-1 is a polynomial of $K[x]$, and the characteristic of K is not a factor of n, then this polynomial has n different roots. There are $\phi(n)$ primitive roots of x^n-1 ; $\phi(n)$ is the number of the positive integers $< n$, which are relatively prime to n. $\phi(n)$ can be calculated by (7, 8). Each root of x^n-1 is a power of every arbitrary primitive root of that polynomial.

[7/3] Let $r_1, r_2, \ldots, r_m$ be the divisors of n which are different from n and $(x^n-1):(x^{r_i}-1)=\psi_i(x)$, then the *h.c.f.* of all $\psi_i(x)$ is a polynomial whose roots are just the primitive roots of $f(x)$. This polynomial is called a *cyclotomic polynomial of order n*; its degree is $\phi(n)$. The method of calculating a cyclotomic polynomial can be shortened by suitable considerations. *E.g.*, the non-primitive roots of $(x^{12}-1)$ are either roots of (x^6-1), or of (x^4-1), the common factor of both polynomials being (x^2-1). Hence the cyclotomic polynomial of order 12 is $((x^{12}-1):(x^6-1)):((x^4-1):(x^2-1)) = (x^6+1):(x^2+1) = x^4-x^2+1$.

Theorem. If α is root of x^n-1, $K(\alpha)$ is a normal extension of K.

Proof. Let α be of order r. If r is not divisible by the characteristic of K, α is a primitive root of x^r-1, and therefore every root of this polynomial belongs to K and from [6/2] it follows that $K(\alpha)$ is normal over K. If $r = p^e r_0$, where $(p, r_0) = 1$, and p is the characteristic of K, then α^{p^e} is a primitive root of $x^{r_0}-1$, and the r_0 different roots of $x^{r_0}-1$ are all powers of α. Hence the theorem holds.

§ 8. GALOIS FIELDS.

[8/1] If Γ is a field containing only a finite numbers of elements, it is said to be a *Galois field*. The prime field has also a finite number of elements, hence the characteristic of Γ is a prime number p. The prime fields (see [2/5]) GF_p of characteristic p are instances of Galois fields. If Γ would contain an element transcendental to GF_p, it should contain an infinite number of elements ; hence Γ is algebraic over GF_p. For the same reason there must exist in Γ a maximum number of elements

$$\alpha_1, \ldots, \alpha_n \qquad (8, 1)$$

which are linearly independent in GF_p, *i.e.*, $\Sigma c_i \alpha_i = 0$. for elements c_i of GF_p, if and only if these elements are all equal to 0. Every element of Γ can be represented in one and only one manner as a linear homogeneous function of the elements (8, 1) with coefficients of GF_p. Hence Γ has p^n different elements, p being the characteristic of Γ, and $n=[\Gamma : GF_p]$.

[8/2] The elements $\neq 0$ of Γ form a multiplicative abelian group A with p^n-1 elements. Let β be an element of A ; then β, β^2, ... cannot be all different. From $\beta^a=\beta^b$ it follows $\beta^{a-b}=1$. Hence each element of A is a root of a cyclotomic equation. Let r be the order of β, hence $\beta, \beta^2, \ldots, \beta^{r-1}, \beta^r=1$ are all different. Let two elements γ and δ be considered as equivalent elements if $\gamma.\delta^{-1}=\beta^i$ then, this equivalence defines a partition of A in classes (see [1/3]). Each class contains r different elements. Let s be the number of the classes, then

$$r.s=p^n-1 \qquad \text{holds.} \qquad (8,\ 2)$$

Hence the order of every element of A is a factor of p^n-1, and therefore every element of A is a root of $x^{p^n-1}-1$. As the polynomial cannot have more than $p-1$ roots, every root is an element of A. So the elements of Γ are identical with the roots of $x^{p^n}-x$, and

$$x^{p^n}-x=\prod_{i=1}^{p^n}(x-\beta_i), \qquad (8,\ 3)$$

where β_i are the elements of Γ.

Let α be a primitive root of $x^{p^n-1}-1$, then

$$\Gamma=GF_p(\alpha) \qquad (8,\ 4)$$

is a normal field over GF_p, because it is the smallest extension admitting the complete reduction of $x^{p^n-1}-1$. From [5/2] it follows, that all Galois fields with p^n elements are isomorphic.

For this reason (8, 4) will also be denoted by

$$GF_{p^n}\ . \qquad (8,\ 4')$$

This field is a smallest extension admitting the complete reduction of (8, 3). Therefore there exists a GF_{p^n} to every prime power p^n. Let α and β be roots of (8, 3) in a field of characteristic p. By making use of the Binomial theorem as in [7/1] we will get the following formulas

$$(\alpha-\beta)^{p^n}=\alpha^{p^n}-\beta^{p^n},$$

$$(\alpha.\beta)^{p^n}=\alpha^{p^n}.\beta^{p^n},$$

and if $\beta\neq 0$,

$$(\alpha:\beta)^{p^n}=\alpha^{p^n}:\beta^{p^n}. \qquad (8,\ 5)$$

Hence the roots form a field GF_{p^n}. These considerations lead us to the following theorem

Theorem. To every power p of a prime number p there exists a Galois field GF_{p^n} of characteristic p, containing p^n elements. $[GF_{p^n}:GF_p]=n$.

Every root of this field is a root of (8, 3). If α is a root of the cyclotomic polynomial of order p^n-1 of $GF_p[x]$, then $GF_{p^n}=GF_p(\alpha)$ holds.

Corollary. If $\gamma_1, \ldots, \gamma_t$ are algebraic to GF_{p^n}, there exists an element γ, so that $GF_{p^n}(\gamma_1, \ldots, \gamma_t)=GF_p(\gamma)$ holds.

Proof. As $GF_{p^n}(\gamma_1, \ldots, \gamma_t)$ is finite over GF_{p^n}, it is a Galois field and is of characteristic p. Hence $GF_{p^n}(\gamma_1, \ldots, \gamma_t)=GF_{p^n}=GF_p(\gamma)$, and as γ cannot belong to GF_{p^n}, the extension $GF_{p^n}(\gamma)$ is identical to the extension $GF_p(\gamma)$.

[8/3] Another interesting property of the Galois fields is given by

Theorem. In a Galois field every irreducible polynomial is separable.

Proof. Let $f(x)$ be an irreducible, but non-separable polynomial in $GF_{p^n}[x]$. From [5/7] it follows that $f(x)=\Sigma a_j x^{jp}$. As $a_j=a_j^{p^n}=b_j^p$, $f(x)=\Sigma b_j^p x^{jp}=(\Sigma b_j x^j)^p$ is reducible, contrary to the supposition.

[8/4] The Galois field has a very close connection with the elementary theory of numbers, and some elementary propositions are nothing else than properties of the G_p.

E.g. The theorem that each element $\neq 0$ of GF_{p^n} satisfy the equation

$$x^{p^n-1}-1=0$$

gives for $n=1$ *Fermat's* theorem

$$x^{p-1}\equiv 1 \quad (\text{mod. p}), \text{ for } x\neq 0. \tag{8, 6}$$

To every element $x\neq 0$ in GF_{p^n} there exists an inverse element $xy=1$, only 1 and -1 are roots of $x^2=1$, and therefore self-inverse; the other elements $\neq 0$ are divided in pairs of inverse elements.

Hence the product of all numbers $\neq 0$ of GF_{p^n} is -1.

In the case $n=1$, we get *Wilson's* theorem (8, 7)

$$(p-1)!\equiv -1 \ (\text{mod. p})$$

Let p be $\neq 2$, $p^n-1=2m$

As $x^{p^n-1}-1=(x^m-1)\quad(x^m+1)$

There are 2 classes of elements $\neq 0$ in $GF_p{}^n$, the mth power of the first class is $+1$, and the mth power of the second is -1. If α is a primitive element of $GF_p{}^n$, the numbers $\alpha, \ldots, \alpha^{2m}=1$ are all different, hence $\alpha^m=-1$, and therefore the odd powers of α are -1, the even powers are $+1$

If $\beta=\gamma^2$, $\beta^m=(\gamma^m)^2=(\pm 1)^2=1$,

Hence every square is an element of the first kind, and every element of the first kind is an even power of α and therefore a square.

The product of two elements of different kind is of the second kind and the product of two elements of same kind is of the first kind. -1 is of the first kind if $(-1)^m-1=0$, *i.e.* if m is even, and it is of the second kind if m is odd.

In the case $n=1$, the elements are classes of residues (mod. p).

(a) is[1] a square if and only if

$x^2 \equiv a$ (mod. p.) has solutions

In this case a is said to de a *quadratic residue* of p; if there is no solution, a is a *quadratic non-residue*.

Using these notations we get the results:

There are $\frac{1}{2}$ $(p-1)$ quadratic residues and $\frac{1}{2}$ $(p-1)$ quadratic non-residues.

The product of a residue and a non-residue is a non-residue.

$x^{\frac{1}{2}(p-1)} \equiv +1$ (mod p) for quadratic residues

-1 ,, ,, ,, ,, non-residues. (8, 8)

-1 is a quadratic residue of the prime numbers $4n+1$

-1 ,, ,, non-residue ,, ,, ,, $4n-1$.

---

[1] See the notation (1, 10).

§ 9. PRIMITIVE ELEMENTS OF SEPARABLE EXTENSIONS.

The proposition of the corollary in [8/2] will be extended for separable extensions of arbitrary fields.

If
$$\Lambda = K(\alpha), \qquad (9, 1)$$
α is said to be a *Primitive element* of the extension Λ over K.

Lemma. Let $f(x)$ and $g(x)$ be polynomials of $K[x]$, let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ and $\beta = \beta_1, \beta_2, \dots, \beta_m$ be their roots respectively; if c is an element of K for which the inequalities
$$\gamma = \alpha + c\beta \neq \alpha_i + c\beta_k \text{ for } k \neq 1 \text{ hold}, \qquad (9, 2)$$
then
$$K(\gamma) = K(\alpha, \beta). \qquad (9, 3)$$

Proof. $\phi(x) = f(\gamma - cx)$ is a polynomial of $K(\gamma)[x]$. Each root λ of $\phi(x)$ must satisfy the condition $\gamma - c\lambda = \alpha_i$, hence β is the only common root of $g(x)$ and $\phi(x)$. As therefore the h. c. f. $(g(x), \phi(x)) = x - \beta$ is a polynomial of $K(\gamma)[x]$, the elements β and $\gamma - c\beta = \alpha$ belong to $K(\gamma)$. Hence every element of $K(\alpha, \beta)$ belong to $K(\gamma)$, and as γ belongs to $K(\alpha, \beta)$, the proposition (9, 3) holds.

Theorem. Let α be algebraic to K, and $\beta, \dots, \kappa$ be roots of separable polynomials of $K[x]$, then there exists in $K(\alpha, \beta, \dots, \kappa)$ a primitive element λ.

Proof. As the theorem holds if K is a Galois field (see [8/2]), we may suppose that K has an infinite number of elements, $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ and $\beta = \beta_1, \beta_2, \dots, \beta_m$ are supposed to be the roots of irreducible polynomials of $K[x]$. From the supposition of the theorem it follows that the roots β_i are all different. An equation $\alpha - \alpha_i + x(\beta - \beta_k) = 0$ has, for $k \neq 1$ atmost one solution. Hence there are in K only a finite number of elements d_{ik}, for which $\alpha + d_{ik}\beta = \alpha_i + d_{ik}\beta_k$ holds. As K has an infinite number of elements, there is an element b, so that $\alpha + b\beta \neq \alpha_i + b\beta_k$, for $k \neq 1$. From the preceding Lemma it follows that $K(\alpha, \beta) = K(\alpha + b\beta)$. By repetition of this procedure we get, after a finite number of steps, a primitive element $\lambda = \alpha + b\beta + \dots + k\kappa$ of $K(\alpha, \beta, \dots, \kappa)$.

Corollary. If K is of characteristic 0, and $\alpha, \beta, \dots, \kappa$ are algebraic to K, then $K(\alpha, \beta, \dots, \kappa) = K(\lambda)$, for a suitably chosen λ.

Proof. In a field of characteristic 0 every polynomial is separable. Hence the existence of a primitive element follows directly from the preceding theorem.

§ 10. SYMMETRIC POLYNOMIALS.

Let K be an arbitrary field. A polynomial $f(x_1, \dots, x_n)$ of $K[x_1, \dots, x_n]$ is said to be a *symmetric polynomial* if $f(x_1, \dots, x_n)$ does not change by any permutation of $x_1, \dots, x_n$. The integral rational functions corresponding to symmetric polynomials (see [3/3]) are said to be *Integral symmetric functions.* [10/1]

As the polynomial $\Pi(x + x_i) = x^n + a_1 x^{n-1} + \dots + a_n$ (10, 1)

does not change by any permutation of the indefinites x_i, the co-efficients

$$a_i = a_i(x_1, \dots, x_n) \tag{10, 2}$$

are symmetric polynomials. These are called the *elementary symmetric polynomials.* We can represent them by

$$a_1 = \Sigma x_k = x_1 + \dots + x_n$$

$$a_2 = \Sigma x_{k_1} x_{k_2}$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$a_i = \Sigma x_{k_1} \dots x_{k_i} \tag{10, 3}$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$a_n = \Sigma x_{k_1} \dots x_{k_n} = x_1 \dots x_n$$

The summation has to be taken over all systems of *different* indices $k_1, \dots, k_i$. Let $f(x) = x_n + b_1 x^{m-1} + \dots + b_m$ be a polynomial of $K[x]$. In a suitable extension of K there is

$$f(x) = \Pi(x - \alpha_k) \quad , \quad \text{hence}$$

$$b_i = (-1)^i a_i(\alpha_1, \dots, \alpha_n) \tag{10, 4}$$

The co-efficients of $f(x)$ are therefore symmetric functions of the roots.

Theorem. Let $f(y_1, \dots, y_n)$ be a polynomial of $K[y_1, \dots, y_n]$, let a_i be the elementary symmetric polynomials, defined by (10, 3), and let $F(x_1, \dots, x_n) = f(a_1, \dots, a_n)$. Then $F(x_1, \dots, x_n)$ is the polynomial 0, only if $f(y_1, \dots, y_n)$ is the polynomial 0.

Proof. In a suitable extension of K, the polynomial $\phi(z) = z^n - y_1 z^{n-1} \pm \dots (-1)^n y_n$ has roots $\alpha_1, \dots, \alpha_n$. Hence

$$F(\alpha_1, \dots, \alpha_n) = f(a_1(\alpha_1, \dots, \alpha_n), \dots, a_n(\alpha_1, \dots, \alpha_n)) = f(y_1, \dots, y_n) \neq 0.$$

As therefore the function F takes values different from *0*, the polynomial *F* cannot be the polynomial *0*.

Corollary. Let the co-efficients of $f(y_1, \dots, y_n)$ be integral numbers and let p be a prime number. Then $f(a_1, \dots, a_n) = F(x_1, \dots, x_n) \equiv 0$ (mod. p) only if the co-efficients of f are congruent to *0* (mod. p).

Proof. The ring $GF_p[x_1, \dots, x_n]$ is homomorphic to the ring of the polynomials in $(x_1, \dots, x_n)$ with integral co-efficients. If $F(x_1, \dots, x_n) \equiv 0$ (mod. p), the corresponding polynomial of $GF_p[x_1, \dots, x_n]$ is the polynomial *0*, hence $f(y_1, \dots, y_n)$ corresponds to the polynomial *0* of $GF_p[y_1, \dots, y_n]$. Therefore the co-efficients of f are divisible by p.

[10/2] *Theorem.* A symmetric polynomial can be represented in one and only one manner as the sum of homogeneous symmetric polynomials of different degrees.

Proof. Every polynomial of $K[x_1, \dots, x_n]$ can be represented as the sum of homogeneous polynomials of the same ring, and we can choose the summands so that the degrees become all different. The difference of two such representations of the same polynomial is a representation of *0* as a sum of homogeneous polynomials of different degrees. Therefore this kind of representation is unique. A homogeneous polynomial becomes transformed by a permutation of the indefinites into a homogeneous polynomial of the same degree; hence a symmetric polynomial is represented as a sum of symmetric homogeneous polynomials.

Let P be a permutation of $1, \dots, n$, and P′ its inverse.

If two monomials

$$x_{i_1}^{a}, \dots, x_{i_n}^{f} \quad \text{and} \tag{10, 5}$$

$$x_{k_1}^{a}, \dots, x_{k_n}^{f} \tag{10, 5'}$$

with the same system of exponents become transformed by P into equal monomials, they will also be transformed by PP′, into equal monomials and therefore the two monomials (10, 5) and (10, 5′) are equal. Therefore the polynomial

$$\Sigma x_1^{a}, \dots, x_n^{f} \tag{10, 6}$$

which denotes the sum of all *different* monomials we get by all permutations of the lower indices of (10, 5) is a symmetric polynomial. By taking the exponents in a non-decreasing order we can represent (10, 6) by

$$[t_1, \dots, t_n] = \Sigma x_1^{t_n} . \, x_2^{t_n + t_{n-1}} . \dots . x_n^{t_n + \dots + t_1} \tag{10, 7}$$

$$t_i \geqq 0 ;$$

The degree of $[t_1, \dots, t_n]$ is

$$m = t_1 + 2t_2 + \dots + nt_n. \tag{10, 8}$$

Theorem. If $f(x_1, \dots, x_n)$ is a homogeneous symmetric polynomial of degree m, it can be represented by

$$f(x_1, \dots, x_n) = \sum_{i=1}^{N} c_i [t_1, \dots, t_n] \tag{10, 9}$$

where c_i are co efficients of f and N is the number of the system of non-negative integers $t_1, \dots, t_n$ satisfying (10, 8).

Proof. As by a suitable permutation of the indefinites x_i each term on the right side of (10. 7) can be transformed in every other, and different terms are always transformed in different ones, either each of these terms occurs as a term of f, or none of them do so. If therefore one of the terms of (10, 7) has in f the co-efficient c_i, then

$$f(x_1, \dots, x_n) - c_i \, [t_1, \dots, t_n]$$

is a symmetric polynomial in $x_1, \dots, x_n$, in which none of the terms of $[t_1, \dots, t_n]$ occurs. When we repeat this procedure with all non-negative integral solutions of (10, 8), we get after N steps 0 represented as the difference of the two sides of the equation (10, 9).

Main theorem of symmetric polynomials. Any symmetric polynomial $f(x_1, \dots, x_n)$ of $K[x_1, \dots, x_n]$ can be represented in one and only one manner by [10/3]

$$f(x_1, \dots, x_n) = F(a_1, \dots, a_n), \tag{10, 10}$$

where a_i are the elementary symmetric polynomials (10, 3), and the co-efficients of F belong to K.

Proof. The symmetric homogeneous polynomials of degree m form a modul M over K (see [5/4]) generated by the polynomials $[t_1, \dots, t_n]$. The rank of M is therefore atmost N. The polynomials

$$a_1^{t_1} . \dots . a_n^{t_n} \tag{10, 11}$$

belong to M, when t_i satisfy (10, 8), and from [10/1] it follows that the N polynomials (10, 11) are independent. Hence they form a basis of M. So every homogeneous symmetric polynomial can be represented by (10, 10), and from the 1st theorem of [10/2] it follows that the same holds for any symmetric polynomial. If there would be two such representations by different $F_1(a_1, \dots, a_n)$ and $F_2(a_1, \dots, a_n)$, then the difference must become 0 contrary to [10/1].

Lemma. The polynomials (10, 7) can be generated by addition and subtraction of polynomials (10, 11).

Proof. Let K be the field of the rational numbers. As every polynomial (10, 7) can be considered as a polynomial of $K[x_1, \dots, x_n]$, it can be represented as a linear homogeneous function of the N polynomials (10, 11) of the same degree. Therefore an equation

$$c[t_1, \dots, t_n] = c_1 \Pi a_i^{r_i} + \dots + c_N \Pi a_i^{s_i}$$

holds, where $\Sigma r_i = \dots = \Sigma s_i = m$, and where $c_1, \dots, c_N$ and $c > 0$ are integers without a common divisor $\neq \pm 1$. Let p be a prime factor of c, then not every c is divisible by p, and

$c_1 \Pi a_i^{r_i} + \dots + c_N \Pi a_i^{s_i} = 0 \pmod{p}$ holds, contrary to the corollary in

[10/1]. Hence $c = 1$, and the lemma holds.

As the elements c_i in (10, 9) are co-efficients of $f(x_1, \dots, x_n)$, the following theorem is a direct consequence of the lemma.

Theorem. The co-efficients of F are elements of the ring generated by the co-efficients of f.

[10/4] For a more detailed investigation of symmetric polynomials the following lemma is useful.

Lemma. Let $i = 1, 2, \dots, n!$, and $f_i(x_1, \dots, x_n)$ be polynomials of $K[x_1, \dots, x_n]$ we get from one of them by the permutations of the indefinites. If each of these polynomials is divisible by every other, they are all of the form

$$D^e . S, \tag{10, 12}$$

where

$$D = \prod_{i<k} (x_i - x_k), \tag{10, 13}$$

$\epsilon = 0, 1$, and S is a symmetric polynomial.

Proof. As the polynomials f_i are all of the same degree, they differ only by factors which are elements of K. Let c_{ik} be the factor which f_1 gets when x_k and x_i become interchanged. To a permutation which we get by carrying out two other permutations one after the other, there corresponds a factor which is the product of the factors corresponding to these two other permutations. To the identical permutation, there corresponds the factor 1. Hence

$$c^2_{ik} = 1,$$

and as any permutation (p, q) of two elements can be expressed by

$(p, q) = (i, p)\,(k, q)\,(i, k)\,(k, q)\,(i, p)$, there is

$$c_{pq} = c_{ip}\,c_{kq}\,c_{ik}\,c_{kq}\,c_{ip} = c^2_{ip}\,c^2_{kq}\,c_{ik} = c_{ik} = \pm 1.$$

Hence either the factors c_{ik} are all $= 1$, then f_1 is a symmetric function, and the lemma holds for $\epsilon = 0$; or the factors c_{ik} are all $= -1$, then f_1 get the factor -1 by odd permutations, and $+1$ by even ones. In this case the polynomial is said to be *alternating*. An alternating polynomial is at the same time symmetric if and only if the characteristic of K is equal to 2. We will suppose that f_1 is alternating and that the characteristic is $\neq 2$. On replacing the indefinite x_k by the value x_i we get a function that does not change by the permutation (i, k).

$F = f_1(x_1, \ldots, x_i, \ldots, x_i, \ldots x_n) = -F$. Hence

$2F = 0$ holds, and as the characteristic is supposed to be $\neq 2$, $F = 0$.

As $f_1(x_1, \ldots, x_n) = (x_k - x_i).\psi(x_1, \ldots, x_n) + F$, the alternating polynomial f_1 must be divisible by $(x_k - x_i)$, and as i, k are arbitrary indices, it is divisible by D. The complementary factor of f_1 is symmetric as it is the quotient of two alternating polynomials. Hence the lemma holds.

Theorem.

$$\mathrm{D} = (-1)^{\frac{1}{2}n(n-1)} \begin{vmatrix} x_1^{n-1} & x_1^{n-2} & \ldots & x_1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_n^{n-1} & x_n^{n-2} & \ldots & x_n & 1 \end{vmatrix} \tag{10, 14}$$

Proof. The determinant is alternating and therefore divisible by D. The other factor is of degree 0, *viz.* both polynomials have the same degree. By comparing the co-efficients of an arbitrary term we get (10, 14).

[10/5] *Theorem.* Let $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ be polynomials of $K[x_1, \ldots, x_n]$, let $(f, g) = 1$ and $f:g$ be symmetric, then f and g are symmetric.

Proof. Let f be transformed into f_1, and g into g_1 by an arbitrary transformation of the indefinites ; then $f.g_1 = g.f_1$. From [4/6] and the supposition of this theorem it follows that f is divisible by f_1 that g is divisible by g_1 and conversely. As this holds for every permutation of the indefinites, it follows from the lemma [10/4] that f and g are symmetric or alternating. If one of them would be alternating, the other must also be alternating, *viz.*, the quotient is symmetric, but in this case the two polynomials should be divisible by D, contrary to the supposition $(f, g) = 1$. Hence f and g are symmetric.

Theorem. Let $F(a_1, \ldots, a_n)$ and $G(a_1, \ldots, a_n)$ be polynomials of $K[a_1, \ldots, a_n]$, a_i being the elementary symmetric polynomials (10, 3) and let $(F, G) = H(a_1, \ldots, a_n)$, $F = f(x_1, \ldots, x_n)$, $G = g(x_1, \ldots, x_n)$, $H = h(x_1 \ldots, x_n)$; then is h an h.c f. of f and g.

Proof. Let $h = (f, g)$. From the preceding theorem it follows that $f:\bar{h}$ and $g:\bar{h}$ are symmetric. Hence $\bar{h}$ is symmetric and can be represented by $\bar{H}(a_1, \ldots, a_n)$. As $\bar{H}$ is a common factor of F and G, it is a factor of H and therefore $\bar{h}$ is a factor of h ; but h is also a factor of $\bar{h}$ *viz.* $\bar{h} = (f, g)$. Hence h and $\bar{h}$ are associated, and the theorem holds.

[10/6] The symmetric polynomials

$$s_t = \sum_{i=1}^{n} x_i^t \qquad (10,\ 15)$$

are called *power sums.*

From (10,15) it follows directly :

$$s_1 = a_1\,, \quad s_{m-1}\, a_1 = s_m + \Sigma x_1^{m-1} x_2$$

$$s_{m-k}\, a_k = \Sigma x_1^{m-k+1} \,.\, x_2 \,.\, \ldots \,.\, x_k + \Sigma x_1^{m-k} \,.\, x_2 \,.\, \ldots \,.\, x_{k+1}$$

$$s_1\, a_{m-1} = \Sigma x_1^2 x_2 \,.\, \ldots \,.\, x_{m-1} + m a_m \,. \quad \text{Hence}$$

$$\sum_{i=1}^{m-1} (-1)^i a_i\, s_{m-i} = -s_m + (-1)^{m-1}\, m a_m \qquad (10,\ 16)$$

Theorem. Let K be a field of characteristic 0, then a_m can be expressed by $s_1, \dots, s_m$ with co-efficients of K, and therefore the symmetric polynomials of K $[x_1, \dots, x_n]$ are polynomials of K $[s_1, \dots, s_n]$.

Proof. $a_1 = s_1$; by mathematical induction we suppose that $a_1, \dots, a_{m-1}$ can be expressed by $s_1, \dots, s_{m-1}$. From (10, 16) it follows that a_m can be expressed by $s_1, \dots, s_m$.

It may be mentioned that this theorem does not hold if K has a characteristic p $\leq$ n and that the elementary symmetric polynomials cannot be expressed with power sums by the help of integral co-efficients only.

Exercise. There is a problem of theory of numbers that it is required to find out sets of integral numbers $a_1, \dots, a_n$ and $b_1, \dots, b_n$ satisfying the conditions

$$a_1 + \dots + a_n = b_1 + \dots + b_n$$

$$a_1^2 + \dots + a_n^2 = b_1^2 + \dots + b_n^2$$

....

$$a_1^m + \dots + a_n^m = b_n^m + \dots + b_n^m \; .$$

Prove that in the case m = n there exist no other solution than the trivial solutions where the a-numbers are identical with the b-numbers.

§11. THE FIELD R (i).

The cyclotomic equation of order 4

$$x^2 + 1 = 0 \qquad (11, 1)$$

is irreducible in R, the field of the rational numbers,

is irreducible in GF_p, if p is a prime number 4n + 3,
viz. -1 is a quadratic non-residue

is reducible in GF_p, if p is a prime number 4n + 1,
viz. -1 is a quadratic residue

is reducible in GF_2 as $(x + 1)^2 = x^2 + 1$ (mod. 2).

We extend R to R (i) by the root i of (11, 1). The elements of R (i) are $r_1 + r_2 i$, r_1 and r_2 being rational numbers.

Let S be the subring of the elements $a + b i$, a, b being integers. As every element of R (i) is of the form $(a + b i) : c$, R (i) is the quotient-field of S.

$r_1 + r_2 i = \alpha$ and $r_1 - r_2 i = \alpha$ are the roots of $x^2 - 2rx + r_1^2 + r_2^2$; α and $\bar{\alpha}$ are said to be *conjugate* elements, and we will use the bar to denote conjugate elements. Further we introduce the *Norm* N (κ) by

$$N(\kappa) = N(\bar{\kappa}) = \kappa\bar{\kappa} = r_1^2 + r_2^2 \qquad (11.\ 2)$$

$N(\alpha)$ is therefore a rational number, and if α is an element $\neq O$ of S

$N(\alpha)$ is a positive integer.

$$\overline{\kappa+\lambda} = \bar{\kappa}+\bar{\lambda}, \quad \overline{\kappa\lambda} = \bar{\kappa}\,\bar{\lambda}$$

$$N(\kappa\lambda) = \kappa\lambda\,\overline{\kappa\lambda} = N(\kappa)\,N(\lambda) \qquad (11,\ 3)$$

$$N(1:\kappa) = 1:N(\kappa)$$

If κ is a unity of S.

$N(\kappa)$ and $1:\ N(\kappa) = 1$

We will denote by

$A_1, A_2, \ldots\ldots$ elements $\neq 0$ of S, then

$A_1 : A_2 = \omega$ is an element of $R(i)$

$\omega = r_1 + r_2 i = (a + b\,i) + (r'_1 + r'_2\,i)$ where a, b are integers

$|r'_1| \leq \frac{1}{2}, |r'_2| \leq \frac{1}{2}$ and

$\omega = A_3 + \omega'$, where $N(\omega') \leq \frac{1}{2}$

$A_1 = A_2 A_3 + A_4$. $A_4 = A_2\,\omega'$, $N(A_4) \leq \frac{1}{2} N(A_2) < N(A_2)$

N has therefore the properties wanted in [4/5].

Hence the elements of S are uniquely factorisable. As $a^2 + b^2 = 1$ has no other solutions with integers a, b than $\pm 1, 0$ and $0, \pm 1$, there are only 4 unities $+1, -1, +i, -i$.

If p and q are prime numbers (*i.e.* prime elements of the ring of the integers), then there are two integers u, v satisfying

$$u\,p + v\,q = 1$$

Hence every common factor of p and q in S is a unity, a prime element of S cannot therefore be a factor of more than one prime number. If a prime element is an integer, it is a prime number if it is of the form $a+bi$, $b \neq 0$, then $a - b\,i$ is a prime element too, *viz.* if $a-bi = A_1\,A_2$, $a + bi = \bar{A}_1\bar{A}_2$.

Hence if π is a prime element but not associated to a prime number, $\pi \bar{\pi} = N(\pi)$ is an integer, and its factors are associated to $1, \pi, \bar{\pi}, N(\pi)$, hence it is a prime number.

In order to know all prime elements of S we have therefore only to see if a prime number is a prime element of S or the product of two prime elements.

(1) $2 = (1+i)(1-i) = i(1+i)^2$, 2 is associated to the square of a prime element

(2) The prime numbers $q = 4n+3$ are prime elements
viz. $N(a+bi) = a^2 + b^2 \equiv 0, 1,$ or $2 \pmod{4}$

(3) The prime numbers $p = 4n+1$ are products of two non-associated prime elements

Proof. As x^2+1 is reducible in GF_p, there is a number d so that $(d+i)(d-i) = d^2+1$ is divisible by p. As none of the factors on the left is divisible by p, p cannot be a prime element in S.

Hence $p = (a+bi)(a-bi)$. If the factors would be associated, either $b = 0, p = a^2$ or $|b| = |a|$, $p = 2a^2$; both cases are impossible. Each prime number p_ι of the form $4n+1$ is therefore a product $\pi_\iota \bar{\pi}_\iota$ and the elements of S are uniquely factorized

$$\mathrm{A} = (-1)^{\epsilon_1}\, i^{\epsilon_2}\, \Pi q_\iota^{k_\iota} . \Pi \pi_\iota^{m_\iota}\, (1-i)^n \qquad , \epsilon_\iota = 0, 1. \tag{11, 4}$$

Hence $$N(A) = \Pi q_\iota^{2k_\iota}\, \Pi p_\iota^{m_\iota}\, 2^n . \tag{11, 5}$$

N (A) is the sum of two squares and every sum of two squares $a^2 + b^2$ can be considered as the norm N $(a+bi)$ of an element of S. By this algebraic consideration we therefore get the following result on theory of numbers.

A number is the sum of two squares if and only if its factorisation is of the form (11, 5).

§ 12. IRREDUCIBILITY OF POLYNOMIALS.

[12/1] In a particular case it is often a difficult task to state whether a given polynomial is irreducible or not. As the notion of irreducibility is fundamental for Algebra, some criteria for irreducibility will be discussed here. They are based on the following theorem.

Theorem. Let S be a ring of unique factorisation, F the quotientfield of S, $f(x)$ a polynomial of $S[x]$ and therefore also a polynomial of $F[x]$. If $f(x)$ is irreducible as a polynomial of $S[x]$ it is also irreducible as a polynomial of $F[x]$.

Proof. Let $f(x)$ be reducible as polynomial of $F[x]$, *i.e.* $f(x) = \phi_1(x)\ \phi_2(x)$, where ϕ_1, ϕ_2 are polynomials of degree > 0, and with coefficients which are quotients of elements of S. By multiplication with a suitable element the polynomials ϕ_1 and ϕ_2 become elements of $S[x]$. Each of these polynomials is the product of an element of S and a primitive polynomial. Hence

$$af(x) = b\ \psi_1(x)\ \psi_2(x)$$

From [4/6].B it follows that $\psi_1(x)$ is a factor of $f(x)$ in $S[x]$. As $\psi_2(x)$ is of the same degree as $\phi_2(x)$, $\psi_1(x)$ should be of smaller degree than $f(x)$. Hence $f(x)$ is reducible in $S[x]$.

This theorem enables us to find out by a finite number of steps, whether a given polynomial in $R[x]$ is irreducible or not, R being the field of all rational numbers. If $f(x)$ is a polynomial of $R[x]$ of degree $m = 2n$, or $= 2n + 1$, there is a rational number r, so that $r f(x) = \phi(x)$ is a primitive polynomial in $S[x]$, S being the ring of the integers. If $\phi(x)$ is irreducible in $S[x]$, it is irreducible in $R[x]$ and then $f(x)$ must also be irreducible in $R[x]$.

If $\phi(x)$ is reducible in $S[x]$, $\phi(x) = \psi(x)\ \psi_1(x)$ and we can suppose without loss of generality that the degree of $\psi(x)$ is $\leq n$. Let $a_0, a_1, \ldots, a_n$ be arbitrary different integers, $\phi(a_i) = \psi(a_i)\ \psi_1(a_i)$, hence $\psi(a_i)$ is a factor of $\phi(a_i)$. Let $\phi(x) = y_0 + y_1 x + \ldots + y_n x^n$, and let

$$g_i^1, \ldots\ldots g_i^{k_i} \text{ be the different factors of } \phi(a_i)$$

The integers y must therefore satisfy one of the following systems of $n + 1$ linear non-homogeneous equations

$$y_0 + a_0 y_1 + \ldots\ldots\ldots\ldots\ldots + a_n^n\ y_n = g_0^{v_0}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_0 + a_n y_1 + \ldots\ldots\ldots\ldots\ldots + a_n^n\ y_n = g_n^{v_n}$$

to every system $v_0, \ldots v_n$, $0 < v_i \leq k_i$ there exists a system of equations, and to every system of equations there exists one solution $(y_0, \ldots, y_n)$ as the determinant of the homogeneous system is $\neq 0$ (see (10, 14)). By the algorithmus of the b.c.f. we are able to find out by a finite number of steps whether one of the polynomials $\Sigma y_i x^i$ is a factor of $\psi(x)$, or not. If none of them is a factor, $\psi(x)$ is irreducible.

By suitable choice of the integers a_i it is sometimes possible to lower the numbers k_i and to make this procedure practicable. We can also use the method of interpolation, which will be explained in a later part of these lectures, instead of solving systems of linear equations. We therefore have only to consider the polynomials $\Sigma y_i x^i$ with integer co-efficients. Although there are some possibilities to simplify the details of this procedure, it becomes often necessary to apply other methods.

[12/2] By [12/1] the problem of irreducibility in a field has been reduced to the corresponding problem in an s. r. o. f. That is important because there is often another ring, homomorphic to the first, and it is sometimes easier to solve the problem of irreducibility in the second ring. There is no possibility of applying this method to fields, because every ring homomorphic to a field is isomorphic with it. We will use this method in order to prove Eisenstein's theorem.

Eisenstein's Theorem. Let $a_0, \dots, a_n$ be integers, $a_0, \dots, a_{n-1}$ be divisible by an arbitrary prime number p, a_n be not divisible by p, and a_0 not by p^2, then $f(x) = a_0 + a_1 x + \dots a_n x^n$ is irreducible.

Proof. We represent, by a homomorphism, the ring of the integers S by GF_p. So $S[x]$ is represented by $GF_p[x]$ and the factorisation in this ring is unique. If $f(x)$ is reducible $f(x) = f_1(x) f_2(x)$, f_1 and f_2 being of degree >0, we get by homomorphism[1]

$$(f(x)) = (a_n x^n) = (a_n)\ (x).\ \dots\ .\ (x) = (f_1(x).(f_2(x)).$$

As (x) is a prime element in $GF_p[x]$,

$$(f_1(x)) = (cx^r),\ f_1(x) = cx^r + pc_1 x^{r-1} + \dots\dots + pc_r$$

$$(f_2(x)) = (dx^t),\ f_2(x) = dx^t + pdx^{t-1} + \dots + pd.$$

Hence $a_0 = p^2 c_r d_t$ in contradiction to the supposition.

We will use the same method for a special case.

$\psi(x) = x^4 + pax^3 - pbx^2 + pcx + d$, p prime number of the type $4m+1$
d quadratic non-residue of p.

We will prove the irreducibility of $\psi(x)$ by proving it in GF_p,
$(\psi(x)) = (x^4 + d)$.

---

[1] See the notation (1, 10).

As -1 is a quadratic residue, there is an integer e, $(e)^2=-1$, $(e)^4=1$ $-d=-1.d$ is a quadratic non-residue. Hence $x^4+d\equiv 0 \pmod{p}$ has no solution and therefore $(\psi(x))=(x^4+d)$, has no factor of degree 1 in GF_p.

If we extend GF_p by a root δ of x^4+d, we get a factorisation

$$x^4+d=\Pi(x-\delta e^{\nu})$$

Each factor of degree 2 has therefore a co-efficient $\delta^2 e^{\nu+\mu}$. As δ^2 does not belong to GF_p, $(\psi(x))$ is irreducible in GF_p. Hence $\psi(x)$ is irreducible in S, and therefore also irreducible in the field R of the rational numbers.

[12/3] *Theorem.* The cyclotomic polynomials are irreducible in the field R of the rational numbers.

Proof. Let n be the order of a cyclotomic equation and n be not divisible by a prime number p. Let

$$f(x)=x^r+a_{r-1}x^{r-1}+\ldots+a_0 \tag{12, 1}$$

be an irreducible factor (with integral co-efficients) of the cyclotomic polynomial and let α be a root of it. $f(x)$ can also be considered as a factor (not necessarily an irreducible one!) of the cyclotomic equation in $GF_p[x]$. Hence there is in GF_{p^*} a primitive root β such that

$$f(\beta)=0, \text{ and therefore}$$

$$0=(f(\beta))^p=\beta^{pr}+a_{r-1}^p\beta^{p(r-1)}+\ldots+a_0^p=\beta^{pr}+a_{r-1}\beta^{p(r-1)}+\ldots+a_0$$
$$=f(\beta^p) \text{ hold.} \tag{12, 2}$$

Let f_1 and f_2 be polynomials with integral co-efficients; then $f_1(\alpha)=f_2(\alpha)$, only if $f_3(x)=f_1(x)-f_2(x)$ is divisible by $f(x)$. In this case $f_3(\beta)=0$, and therefore $f_1(\beta)=f_2(\beta)$. Hence by the correspondence

$$\Sigma b_i\alpha^i \longrightarrow \Sigma b_i\beta^i,\ b_i \text{ being integers,} \tag{12, 3}$$

there corresponds to every element of the ring generated by α, one and only one element of $GF_p(\beta)$. As in (12, 3) the addition and the multiplication hold, the correspondence is a homomorphism. α^i corresponds to β^i, where $1\leq i\leq n$; but, as these n powers of β are all different, β^i is conversely homomorphic to no other power of α than α^i. As the roots of $f(x)$ in $R(\alpha)$ are all powers of α, and these roots correspond to the roots of $f(x)$ in $GF_p(\beta)$, the root homomorphic to β^p (see(12, 2)) must be α^p. Hence: if α is a root of $f(x)$, α^p is also a root of $f(x)$. The same holds for

α^{pq}, when the prime number q is not a factor of n, and generally for α^m, if $(m, n)=1$. Hence every primitive root of x^n-1 is a root of $f(x)$. The irreducible polynomial $f(x)$ is therefore identical with the cyclotomic polynomial.

Remark. Although the proof of this theorem has been done by the help of GF_p the theorem itself does not generally hold in GF_p. There are cyclotomic polynomials which are reducible in every GF_p. It may be helpful to consider an example of this kind.

$n=8$; cyclotomic equation x^4+1. Primitive roots: $\alpha, \alpha^3, \alpha^5, \alpha^7$.

1. $p=2$. $x^4+1\equiv(x+1)^4 \pmod{2}$; roots $\alpha=1=\alpha^4$.

2. $p=4n+1$. $-1\equiv d^2 \pmod{p}$ (see [8/4])

$$x^4+1\equiv(x^2-d)\,(x^2+d) \pmod{p}$$

$$\equiv(x^2-2)\,(x^2+2) \pmod{5};\ \text{roots } [\beta, \beta^5];\ [\beta^3, \beta^7].$$

$$\equiv(x-2)\,(x+2)\,(x-8)\,(x+8) \pmod{17};$$

$$\text{roots } 2;\ 2^5;\ 2^3;\ 2^7.$$

3. $p=4n+3$. -1 is a quadratic non-residue, hence either 2 or -2 is a quadradic residue. So there are 2 different cases:

a. $2\equiv s^2 \pmod{p}$

$$x^4+1\equiv(x^2+sx+1)\,(x^2-sx+1) \pmod{p}$$

$$\equiv(x^2+3x+1)\,(x^2-3x+1) \pmod{7}\ \text{roots } \beta, \beta^7;\ \beta^3, \beta^5.$$

b. $2\equiv-t^2$ (mod. p.)

$$x^4+1\equiv(x^2+tx-1)\,(x^2-tx-1) \pmod{p}$$

$$\equiv(x^2+x-1)\,(x^2-x-1) \pmod{3}\ \text{roots } \beta, \beta^3;\ \beta^5, \beta^7.$$

From this example we realise that it is not possible to give the proof of the preceding theorem by the help of one homomorphism only, as it has been done in the proof of Eisenstein's theorem. On repeating the general proof in the special case $n=8$, the considerations mod. 3, mod. 5, and mod. 7 show that if the primitive root α is a root of any polynomial in $R[x]$, then $\alpha^3, \alpha^5, \alpha^7$ respectively (*i e.*, every primitive root of the cyclotomic equation) is a root of that polynomial.

Theorem. Let K be an arbitrary field not containing the indefinites $x_1^1, \dots, x_n^n$ and let $n>0$, then the determinant $X=\det(x_i^j)$ is an irreducible polynomial of $K[x_1^1, \dots, x_n^n]$. [12/4]

$a_n \neq 0$ an arbitrary polynomial of odd degree n,

$$\text{let } t = \left|\frac{a_0}{a_n}\right| + \left|\frac{a_1}{a_n}\right| + \dots + \left|\frac{a_{n-1}}{a_n}\right| + 1,$$

$$\frac{1}{a_n} f(t) \geqq t^n - \left\{\left|\frac{a_0}{a_n}\right| + \dots + \left|\frac{a_{n-1}}{a_n}\right| t^{n-1}\right\} \geqq t^n - t^{n-1}(t-1) > 0$$

$$\frac{1}{a_n} f(-t) \leqq -t^n + \left\{\left|\frac{a_0}{a_n}\right| + \dots + \left|\frac{a_{n-1}}{a_n}\right| t^{n-1}\right\} \leqq -t^n + t^{n-1}(t-1) < 0$$

$f(t)$ and $f(-t)$ have opposite signs, and as the function represented by the polynomial $f(x)$ is continuous, there must be a real number x_0, so that $f(x_0)=0$. The polynomials of odd degree of $K[x]$ have therefore a root in K.

If $a>0$, then $\sqrt{a}$ exists. Let i be a root of x^2+1, $\Lambda = K(i)$.

$\alpha = a+bi$ an arbitrary element of Λ, $c = \sqrt{a^2+b^2}$, then

$\{\sqrt{\tfrac{1}{2}} \ (\sqrt{c+a} + i\sqrt{c-a})\}^2 = \alpha + bi$, if we choose the signs of the roots on the left side in a suitable manner. Hence each element of Λ is the square of an element of Λ. The well known method of solving an equation of degree 2 by the help of square roots is therefore applicable. Hence the suppositions made in [18/1] hold if K is the field of all real numbers and Λ the field of the complex numbers. In other words:

Fundamental Theorem of Classical Algebra. The field of the complex numbers is closed.

Corollary. Every algebraic extension of the field K of the real number is isomorphic to K(i).

Proof. Let Λ be an algebraic extension of K and α an element of Λ not belonging to K. As α is a root of a polynomial of $K[x]$, $K(\alpha)$ is isomorphic to a subfield of K (i) different from K, and as $[K(i):K)]=2$, $K(\alpha)$ is isomorphic to K(i). Hence $K(\alpha)$ is closed; every element algebraic to $K(\alpha)$ must be an element of $K(\alpha)$. Hence $\Lambda = K(\alpha)$.

§ 14. SOLUTIONS OF ALGEBRAIC EQUATIONS.

In [5/3] it has been proved that every polynomial has roots, *i.e.*, that every algebraic equation has a *solution*. We also learned to construct suitable fields in which such solutions exist and to find out the solutions in them. The simplest way is, to construct a field whose elements are classes of residues, then the class containing the polynomial x is a solution. [14/1]

Although this method is simple, and the result is very important for some algebraic investigations, it is nearly useless for other purposes, *e.g.*, for applied Mathematics. The solution which is required, is mostly not an arbitrary one, but a solution in a given field, sometimes in a certain part of a given field, sometimes also in a given set of fields. For dealing with these problems we have got a valuable hint for the fundamental theorem of §13 that every equation with complex co-efficients has solutions which are complex numbers. But the proof given in §13 does not show any way to find out these solutions. As there cannot exist a complete list of all complex numbers, the "finding out" is nothing else than the statement that the solution which we require is identical with a complex number defined in another manner which seems to be more simple and appropriated to the special problem.

For the purpose of an analytic problem a convergent procedure leading to the solution may be required. In applied Mathematics it is mostly sufficient to state that there is a solution in a well defined domain of the complex plane whose diameter is smaller than a certain number depending on the accuracy. Methods of finding out the approximate value of the solutions, will be given in another part of these lectures.

For Algebra and its applications to Geometry it is important to know if the solution of an equation can be done by solving several equations of special types, *e.g.*, by extracting roots. A complete analysis of the possibility and the methods of such a reduction is the task of *Galois' theory*. This theory will not be done in these lectures. We only will consider some interesting examples.

Without any loss of generality we can suppose that the equation is given by [14/2]

$$y^n + b_{n-1}\, y^{n-1} + \dots + b_1 y + b_0 = 0 \qquad (14.1)$$

$$-b_{n-1} = \beta_1 + \dots + \beta_n.$$

Let K be the field of the co-efficients. If the characteristic of K is not a factor of n, *e.g.*, if the characteristic is 0, we can make the substitution $x = y + \frac{b_{n-1}}{n}$, and we get an equation for x in K. The roots of this equation are $\alpha_i = \beta_i + \frac{b_{n-1}}{n}$. Hence $\Sigma\alpha_i = 0$.

There is therefore no loss of generality in these cases to suppose that the equation is given by

$$x^n + a_{n-2}x^{n-2} + \ldots + a_0 = 0. \qquad (14,\ 2)$$

[14/3] Let $n = 2$, $x^2 + a = 0$ (14, 3)

The solution is done by extracting a square root. Every field K′ containing K and one root of an equation of degree 2 contains also the second root; hence K′ contains a normal field over K. The reduction to (14, 3) is not possible if the characteristic of K is equal to 2. In GF_2 there exists one irreducible polynomial of degree 2 namely $f(x) = x^2 + x + 1$. The classes of residues (0), (1), (x), $(x+1)$ may be denoted by

$$0,\ 1,\ \alpha,\ \beta.$$

The addition and multiplication in $GF_2(\alpha) = \mathrm{K}$ is given by the following matrices:

Matrix of addition

$$(a^i_k) = \begin{pmatrix} 0 & 1 & \alpha & \beta \\ 1 & 0 & \beta & \alpha \\ \alpha & \beta & 0 & 1 \\ \beta & \alpha & 1 & 0 \end{pmatrix} \qquad a^i_j + a^j_k = a^i_k \qquad (14,\ 4)$$

Matrix of multiplication

$$(b^i_k) = \begin{pmatrix} 1 & \alpha & \beta \\ \alpha & \beta & 1 \\ \beta & 1 & \alpha \end{pmatrix} \qquad b^i_j \cdot b^j_k = b^i_k \qquad (14,\ 5)$$

Both the elements of GF_2 are squares of elements of GF_2 and therefore it is not possible to solve the equation given by the irreducible polynomial of degree 2 in $GF_2[x]$ by extracting square roots.

[14/4] Let $n = 3$. $f(x) = x^3 + px + q$. The characteristic of K is supposed to be $\neq 2, 3$.

A field containing the three roots α_1, α_2, α_3 of $f(x)$ contains also

$$(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \delta = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 - \alpha_1^2\alpha_3 - \alpha_2^2\alpha_1 - \alpha_3^2\alpha_2$$

δ^2 is a symmetric function of a_1, a_2, a_3 and therefore an element of K.

$$f'(x)=(x-a_2)\ (x-a_3)+(x-a_1)\ (x-a_3)+(x-a_2)\ (x-a_3)$$

$$f'(a_1)=(a_1-a_2)\ (a_1-a_3)$$

$$\delta : f'(a_1)=a_2-a_3 \qquad a_2=\tfrac{1}{2}[-a_1+\delta : f'(a_1)]$$

hence

$$a_1=-a_2-a_3 \qquad a_3=\tfrac{1}{2}[-a_1-\delta : f'(a_1)]$$

K (δ) is therefore a normal field, K $(a_1, a_2, a_3)=$ K (a_1, δ),

$$[K(a_1, \delta) : K(\delta)]=3$$

It is possible to get the roots of the equation from K $(\delta, \sqrt{-3})$ by extracting cube roots only. Let ρ and ρ^2 be the roots of the cyclotomic equation

$$x^2+x+1=0, \text{ hence } \rho=-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{-3},\ \rho^2=-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{-3}$$

ρ has been plac
instead of ω

It is easy to show by calculations that $(\rho, a)=a_1+\rho a_2+\rho^2 a_3$ and $(\rho^2 a)=a_1+\rho^2 a_2+\rho a_3$ are cube roots of elements of K $(\delta, \sqrt{-3})$.

$$(\rho, a)^3=A+B\sqrt{-3},\ A=\Sigma a_1^3-\tfrac{3}{2}\Sigma a_1^2 a_2+6a_1a_2a_3,\ B=\tfrac{3}{2}\delta.$$

A is a symmetric function and therefore an element of K. On making use of the fact that $a_1+a_2+a_3=0$ we can easily calculate

$A=-\dfrac{27}{2}q$. On interchanging ρ and ρ^2, *i.e.*, on interchanging $\sqrt{-3}$ and $-\sqrt{-3}$ we get $(\rho^2, a)^3$ Hence $(\rho, a)^3=-\dfrac{27}{2}q+\tfrac{3}{2}\delta\sqrt{-3}$

$$(\rho^2, a)^3=-\frac{27}{2}q-\tfrac{3}{2}\delta\sqrt{-3}$$

In the same manner we calculate:

$$(\rho, a)\ (\rho^2, a)=\Sigma a_1^2+(\rho+\rho^2)\ (a_1a_2+a_1a_3+a_2a_3)$$

$$=\Sigma a_1^2-(a_1a_2+a_1a_3+a_2a_3)$$

$$=(a_1+a_2+a_3)^2-3(a_1a_2+a_1a_3+a_2a_3)=-3\,p.$$

On extracting the cube root of a number, a factor 1, ρ, ρ^2 is arbitrary.

If we extract the roots $(\rho, \alpha) = \sqrt[3]{\frac{27}{2}q + \frac{3}{2}\delta\sqrt{-3}}$

$$(\rho^2, \alpha) = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\delta\sqrt{-3}}$$

we have to take these two arbitrary factors in such a manner, that

$$(\rho, \alpha)(\rho^2, \alpha) = \sqrt[3]{\frac{27}{4}q^2 + \frac{27}{4}\delta^2} = -3\sqrt[3]{p^3}$$

becomes $-3p$, and not $-3\rho p$ or $-3\rho^2 p$. Therefore one factor can be arbitrarily chosen. If we select it and get so

$(\rho,\alpha)=\kappa$, $(\rho^2,\alpha)=\lambda$, the other possibilities are

$(\rho,\alpha)=\rho\,\kappa$, $(\rho^2,\alpha)=\rho^2\lambda$

$(\rho,\alpha)=\rho^2\,\kappa$, $(\rho^2,\alpha)=\rho\lambda$. We get $\alpha_1, \alpha_2, \alpha_3$ by

$$(\rho,\alpha)+(\rho^2\alpha)=2\alpha_1+(\rho+\rho^2)\;(\alpha_2+\alpha_3)=3\alpha_1$$

$$\rho^2\,(\rho,\alpha)+\rho\,(\rho^2,\alpha) \qquad =3\alpha_2$$

$$\rho\,(\rho,\alpha)+\rho^2\,(\rho,\alpha) \qquad =3\alpha_3$$

Different choices of the arbitrary factor of (ρ, α) give us only a permutation of the roots.

[14/5] Let $n=4$. $x^4+px^2+qx+r=0$

the characteristic of K is supposed to be $\neq$ 2, 3

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots in a suitable extension

$$\beta_1=-(\alpha_1+\alpha_2)\;(\alpha_3+\alpha_4)$$

$$\beta_2=-(\alpha_1+\alpha_3)\;(\alpha_2+\alpha_4)$$

$$\beta_3=-(\alpha_1+\alpha_4)\;(\alpha_2+\alpha_3).$$

As by the permutations $(\alpha_1, \alpha_2), (\alpha_3, \alpha_4), (\alpha_1, \alpha_3), (\alpha_2, \alpha_4), (\alpha_1, \alpha_4) (\alpha_2, \alpha_3)$ $\beta_1, \beta_2, \beta_3$ are only interchanged, by an arbitrary permutation of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ the elements $\beta_1, \beta_2, \beta_3$ are interchanged too, hence a symmetric function of $\beta_1, \beta_2, \beta_3$, is not changed and therefore it is a symmetric function of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. There exists therefore an equation $x_3 + b_1x^2 + b_2x + b_3 = 0$ with elements from K having the roots $\beta_1, \beta_2, \beta_3$.

By an easy calculation we find

$$b_1 = +2p_1, \quad b_2 = p^2 - 4\,r, \quad b_3 = -q^2$$

It is therefore possible to find out $\beta_1, \beta_2, \beta_3$ by extracting roots only, In order to find out $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, we have to consider that

$$(\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = 0, \qquad (\alpha_1 + \alpha_2)\ (\alpha_3 + \alpha_4) = -\beta_1$$

hence $\alpha_1 + \alpha_2$ and $\alpha_3 + \alpha_4$ are the roots of $x^2 - \beta_1 = 0$

$$\alpha_1 + \alpha_2 = \sqrt{\beta_1}, \qquad \alpha_3 + \alpha_4 = -\sqrt{\beta_1}$$

in the same manner we get

$$\alpha_1 + \alpha_3 = \sqrt{\beta_2}, \qquad \alpha_2 + \alpha_4 = -\sqrt{\beta_2}$$

$$\alpha_1 + \alpha_4 = \sqrt{\beta_3}, \qquad \alpha_2 + \alpha_3 = -\sqrt{\beta_3}$$

For every root a factor ± 1 remains indefinite, but as

$$\sqrt{\beta_1\beta_2\beta_3} = \sqrt{q^2} = (\alpha_1 + \alpha_2)\ (\alpha_1 + \alpha_3)\ (\alpha_1 + \alpha_4)$$

$$= \alpha_1^2\ (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) + \Sigma\alpha_i\ \alpha_k\ \alpha_l = -q$$

only two of the factors are arbitrary. The choice of these factors corresponds to a permutation of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ as it is seen from the final formulas:

$$2\alpha_1 = \sqrt{\beta_1} + \sqrt{\beta_2} + \sqrt{\beta_3} \qquad 2\alpha_3 = -\sqrt{\beta_1} + \sqrt{\beta_2} - \sqrt{\beta_3}$$

$$2\alpha_2 = \sqrt{\beta_1} - \sqrt{\beta_2} - \sqrt{\beta_3} \qquad 2\alpha_3 = -\sqrt{\beta_1} - \sqrt{\beta_2} - \sqrt{\beta_3}\ .$$

When we exclude the cases of characteristic 2 and 3, the equations of degree ≤ 4 can therefore be solved by extracting roots only. For equations of higher degree, only in special cases the solutions can be found out by extracting roots. A proof of this very interesting fact will not be given in this course of lectures.